

Defense Science Board
2003 Summer Study

on

**DoD Roles and Missions in
Homeland Security**



VOLUME I

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

November 2003

**Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140**

This report is a product of the Defense Science Board (DSB).

The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions and recommendations in this report do not necessarily represent the official position of the Department of Defense.

This report is unclassified.



OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR THE ACTING UNDER SECRETARY OF DEFENSE
(ACQUISITION, TECHNOLOGY & LOGISTICS)

SUBJECT: Report of the Defense Science Board 2003 Summer Study on DoD
Roles and Missions in Homeland Security, Volume I

I am pleased to forward the final report of the DSB 2003 Summer Study on DoD Roles and Missions in Homeland Security. The report evaluates DoD's role in homeland security and makes recommendations on how best to accomplish this mission.

The conceptual thinking and the capabilities required to address the homeland security challenge are still immature. The study concludes that maturing the conceptual framework and capabilities related to homeland protection will require a holistic approach. Thus, fostering a holistic approach to protecting the homeland is a guiding theme for this study. The report's recommendations, which fall into the following six areas, reflect this theme.

- Global situation awareness
- Protect DoD mission-critical infrastructure
- Deter and prevent attack
- Emergency preparedness and incident response
- Exporting DoD core competencies
- Empowering U.S. Northern Command

I endorse all of the recommendations of the Task Force and encourage you to review their report.

A handwritten signature in black ink, reading "William Schneider, Jr.", is located below the text of the endorsement.

William Schneider, Jr.
Chairman

This page intentionally left blank



DEFENSE SCIENCE
BOARD

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

MEMORANDUM FOR THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Report of the Defense Science Board 2003 Summer Study on DoD
Roles and Missions in Homeland Security, Volume I

Developing an effective capability to protect the homeland is a top national priority. It is also a complex undertaking filled with many challenges. There are so many assets to protect, so many modes of attack available to adversaries, and so many organizations involved, that, understandably, both the conceptual thinking and the capabilities required are still immature. Maturing the conceptual framework and capabilities related to homeland security, the DSB believes, requires a holistic approach—a guiding theme for this study.

This report identifies capabilities and initiatives needed by DoD to fulfill its responsibilities to project force when directed and to protect the homeland. It focuses on those capabilities that depend upon DoD working closely with other agencies. In addition, opportunities are identified for DoD to "export" some of its core competencies to help accelerate the maturation of the many agencies involved in homeland security tasks.

The principal findings and recommendations fall in six key areas:

- Information is vital to homeland security. *Yet improvements are needed in many areas of information sharing, assurance, and collection.* First, incentives are needed to enhance information sharing. Second, tools and capabilities for information assurance need to be developed and implemented. Third, collection capabilities, importantly in the area of human intelligence, must be enhanced. In general, foreign intelligence collection must be more proactive and better integrated with domestically derived intelligence.
- DoD's ability to fulfill its missions—most notably force projection—is dependent on an intricate infrastructure in the United States. *DoD is not doing enough to address the*

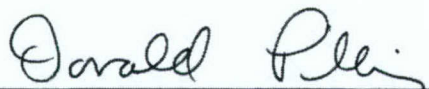
vulnerabilities of mission critical infrastructure and services, particularly in areas outside its direct control. A systematic approach—that focuses both “inside and outside the fence”—must be taken to identify and redress vulnerabilities. Moreover, cyber security and cyber-based aspects of critical infrastructure need to be better integrated into DoD mission-critical infrastructure protection efforts.

- *Ocean vessels, cruise missiles, and low-flying aircraft are credible delivery systems available to adversaries. DoD needs to take steps to counter these threats as a complement to ongoing initiatives to defend against ballistic missiles. First, much more can and should be done to improve maritime security and to integrate maritime-security capabilities across the federal government. Second, because these delivery systems could threaten the continental United States with biological and other weapons of mass destruction, DoD should create a master plan for defense against the low-altitude air threat.*
- *Should the U.S. homeland be attacked, DoD could be called on to assist with incident response. Execution of this mission could require capabilities in areas where the Department is deficient: 1) mitigation and remediation of the effects of attacks from weapons of mass destruction, 2) the ability to surge medical capabilities, 3) communication operability between first responders and federal, state, and local agencies. The report offers detailed recommendations for improving capabilities in each of these areas as well as enhancing Reserve Component capabilities that can support the homeland security mission.*
- *DoD can enhance homeland security by “exporting” relevant core competencies that match the needs of other organizations that have homeland security responsibilities. The study identifies three core competencies in particular: training, experimentation, and operational-level planning and execution. Responsibility to develop, and oversee execution of, plans to export core competencies to other agencies should be assigned to U.S. Northern Command.*

- *U.S. Northern Command must be empowered for the nation to achieve its homeland security and homeland defense goals. The study recommends more than a dozen new tasks for NORTHCOM, with four identified as priorities: develop a roadmap for maritime surveillance; develop a roadmap for defense against the low-altitude air threat; assume operational lead for DoD mission-critical infrastructure protection in CONUS; and assume the lead for exercises, training, experiments, and standards related to homeland defense and military assistance to civil authorities.*

The specific recommendations provided in the pages that follow reflect the holistic approach to protecting the homeland that the DSB envisions for the Department of Defense. By taking this approach, and developing the capabilities described in the six areas above, the security of our nation will be improved.


Donald Latham, Co-Chair


ADM Donald Pilling, USN (Ret), Co-Chair

This page intentionally left blank

TABLE OF CONTENTS

EXECUTIVE SUMMARY	iii
CHAPTER 1. INTRODUCTION	1
Scope	1
Study Approach	2
CHAPTER 2. GLOBAL SITUATION UNDERSTANDING	7
Share and Assure Information	8
Improve Information Collection and Analysis	18
Information: A Critical Enabler	22
CHAPTER 3. PROTECT DOD MISSION-CRITICAL INFRASTRUCTURE	25
Critical Challenges Lie "Outside the Fence"	25
Current Activities	28
The Cyber Threat	31
The Defense Industrial Base	33
What DoD Needs to Do	34
CHAPTER 4. DETER AND PREVENT ATTACK	39
Extend Maritime Defense	40
Defend Against the Low-Altitude Air Threat	49
North American Defense Command	52
CHAPTER 5. EMERGENCY PREPAREDNESS AND INCIDENT RESPONSE	57
Defend Against CBRNE Attacks	57
Create a Medical Surge Capability	66
Improve Communications Operability	71
Enhance National Guard Capabilities	74
CHAPTER 6. EXPORTING DOD CORE COMPETENCIES	79
Training	79
Experimentation	79
Operational-Level Planning and Execution	80
Making it Happen	81
CHAPTER 7. AN EVOLVING ROLE FOR NORTHCOM	83
CHAPTER 8. IN CONCLUSION	85
APPENDIX I. TERMS OF REFERENCE	87
APPENDIX II. MEMBERSHIP	89
APPENDIX III. PRESENTATIONS TO THE TASK FORCE	93

*TABLE OF CONTENTS*_____

APPENDIX IV. REFERENCES.....	99
APPENDIX V. GLOSSARY OF ACRONYMS AND ABBREVIATIONS.....	103

EXECUTIVE SUMMARY

The United States faces stealthy adversaries who have demonstrated both motives and means to inflict grave damage on the U.S. homeland. The nation's strategy in response to this type of adversary is clear: engage the threat as far as possible from the U.S. homeland, on its turf. This approach requires a multi-agency government effort, with the Department of Defense (DoD) playing a major role.

A capability to protect the homeland is a necessary complement to the capability of strategic reach against these asymmetric threats. However, the challenges of homeland protection are complex. There are so many assets to protect, so many modes of attack available to adversaries, and so many organizations (federal, state, local, and private) involved that, understandably, both the conceptual thinking and the capabilities required are still immature.

Responsibilities and authorities must be assigned and operative terms (homeland defense and homeland security, for example) need to be defined. The Defense Science Board (DSB) read with care current definitions and wrestled with inventing new ones. In the end, instead of focusing on precise distinctions between various terms, the board adopted a broad framework, consistent with the study terms of reference, within which to consider homeland protection issues.

Maturing the conceptual framework and capabilities related to homeland protection, the DSB believes, requires a holistic approach. However, organizational boundaries inhibit such an approach. Thus, fostering a holistic approach to protecting the homeland is a guiding theme for this study and the recommendations reflect this theme.

This study identifies capabilities and initiatives needed by DoD to fulfill its responsibilities to project force when directed and to protect the homeland. Further, it focuses on those capabilities that depend upon DoD working closely with other agencies. In addition, opportunities are identified for DoD to "export" some of its core

competencies in order to accelerate the maturation of the Department of Homeland Security.

The principal findings and recommendations fall in six key areas, described in turn below.

GLOBAL SITUATION AWARENESS

Today, more than ever, information is vital to homeland security. It is a key to understanding the adversary and to developing an effective awareness of the global security environment. The DSB focused on two aspects of the challenge to improve information sharing, assurance, and collection. First, it studied how to gain the widely recognized benefits of increased information sharing while managing its associated risks. Second, it considered how to enhance human intelligence collection, arguably the most critical source of information in the war on terrorism.

The DoD—and the U.S. government—still lack an effective approach to reaping the benefits of information sharing within and among agencies while assuring the integrity, availability and confidentiality of information. Incentives are needed to enhance information sharing, and tools and capabilities for information assurance must be developed and implemented. DoD (and the U.S. government as a whole) must

- Motivate individuals to share information more effectively. Use incentives to change organizational cultures such that former “owners” of information become stewards for all potential users.
- Get security policy right. Information must be protected *and* shared at the same time. Better information-assurance tools are needed in support of this policy. The required tools include better techniques for discovering system weaknesses, designing effective defenses, and developing consistent metrics to evaluate the impact of compromise to systems.

- Make information technology architectures converge to facilitate and standardize sharing capabilities. The goal is to *share knowledge* in order to jointly achieve common goals that are unattainable by individuals or single departments or agencies. Engage the federal U.S. Chief Information Officers Council.

Information sharing depends on having information of value; thus collection and analysis are critical elements in the equation. There are still unexploited opportunities to make human intelligence a more potent contributor to the understanding of the threat.

- DoD should establish a more robust defense human intelligence (HUMINT) capability than exists today. The Defense HUMINT Service must be reinvented to provide clandestine battlefield support and augmented technical collection. These capabilities will require improvements in both human-derived and technical capabilities.
- DoD must take the fight to the adversaries proactively – into the “badlands” and other sanctuaries. DoD needs to place operatives in areas where terrorists are known to exist.
- DoD needs to improve technical collection and close access to adversaries. Improve capabilities for evaluating and protecting new sources, methods and concepts and improving capabilities for penetrating hard targets.
- These are appropriate areas to revitalize defense human intelligence and link naturally to requisite improvements for intelligence, surveillance and reconnaissance (ISR) capabilities.
- Domestically derived intelligence and foreign intelligence need to be more effectively integrated to ensure homeland security. Sharing between these communities can extend beyond analysis and

information to include systems engineering, architecture skills, technologies and methodologies.

- Upgrades are needed in all areas of intelligence collection. In addition, the analytic component of intelligence needs to be more highly integrated with collection.

PROTECT DoD MISSION-CRITICAL INFRASTRUCTURE

DoD's ability to fulfill its missions — most notably force projection — is dependent on an intricate infrastructure in the United States. The majority of this infrastructure is not owned or controlled by DoD or the federal government, but by the private sector or state and local governments. DoD mission-critical infrastructure encompasses many diverse pieces and functions: military bases, transportation, communication, power, fuel, food, ammunition, other logistics, and the defense industrial base. Both physical and cyber attacks on this infrastructure are of concern, and there is potential for "single-point failures."

While some good work is being done in response to the critical infrastructure problem, overall DoD must do more to address the vulnerabilities of mission-critical infrastructure and services, particularly in areas outside of its direct control.

A systematic approach must be taken to identify and redress vulnerabilities of the infrastructure critical to DoD's mission, with lead operational responsibilities assigned to the Assistant Secretary of Defense for Homeland Defense and U.S. Northern Command (NORTHCOM). The Under Secretary of Defense for Acquisition Technology and Logistics needs to address defense-industrial-base vulnerabilities. Activities such as those at the U.S. Pacific Command and Camp Lejeune, North Carolina, described in the body of this report, provide examples of civilian-military cooperation for emergency response and critical infrastructure protection that have wider relevance.

Capabilities and tools to support a systemic approach to DoD mission-critical infrastructure protection, such as exist at the Joint Program Office-Special Technical Countermeasures (JPO-STC) should be expanded and made available to other government agencies. The JPO-STC should be assigned to NORTHCOM. Each combatant command should fully implement Appendix 16 to their operations plans and ensure that a strong military-civilian effort is developed.

Finally, cyber security and cyber-based aspects of critical infrastructure need to be better integrated into DoD mission-critical infrastructure protection efforts, which have largely focused on physical attacks. Despite increased investment and awareness, information technology and systems remain vulnerable to cyber attacks. The United States Strategic Command needs to be engaged in addressing cyber-security challenges, with the Defense Advanced Research Projects Agency and the National Security Agency providing necessary supporting research.

DETER AND PREVENT ATTACK

Ocean vessels, cruise missiles and low-flying aircraft are credible delivery systems available to adversaries. DoD needs to take steps to counter these threats as a complement to ongoing initiatives to defend against ballistic missiles.

First, much more can and should be done now to improve and integrate DoD's maritime ISR assets with the improved maritime indications and warning capabilities being fielded by the Department of Homeland Security, Department of Transportation, Central Intelligence Agency, and Federal Bureau of Investigation. Collectively, these DoD and non-DoD assets could provide the nation with a robust capability to identify, track, and, where appropriate, intercept suspicious cargo and vessels as far from U.S. shores as possible. The U.S. Navy, U.S. Northern Command, and the U.S. Coast Guard should be assigned active roles in the operation of this national maritime-surveillance system-of-systems, which should be

designed to provide a forward line of defense against cruise missiles and other low-altitude threats.

Second, because these delivery systems could threaten the continental United States (CONUS) with biological and other weapons of mass destruction, the DoD (i.e., North American Aerospace Defense Command [NORAD], working with U.S. Northern Command and the Joint Theater Air and Missile Defense Organization) should create a master plan for defense against the low-altitude air threat (an activity that began at the conclusion of the DSB deliberations on this study). The Under Secretary of Defense for Acquisition, Technology and Logistics should be tasked to translate this master plan into a supporting technology development and acquisition plan. Although no new DoD program office is warranted at this time, the Office of the Secretary of Defense should ensure that DoD's maritime ISR requirements are included in the Space Based Radar development program.

In order to effectively operate the capabilities described, and provide integration between air and maritime defense, the DSB recommends possible creation of a North American Defense Command, which would evolve out of today's NORAD.

EMERGENCY PREPAREDNESS AND INCIDENT RESPONSE

DoD's role in homeland security extends beyond homeland defense to include military support to civil authorities. Should the U.S. homeland be attacked, DoD could be called on to assist with incident response. Execution of this mission could require capabilities in several areas that need increased emphasis and priority in funding:

- Mitigation and remediation of the effects of attacks from chemical, biological, nuclear, radiological, or high-explosive (CBRNE) weapons
- The ability to surge medical capabilities
- Communication operability between first responders and federal, state, and local agencies

involved in emergency preparedness and incident response

Moreover, the Reserve Components have many capabilities that should be enhanced and can support the homeland security mission.

CBRNE Attacks. Detecting, identifying, and localizing devices or materials across the chemical, biological, radiological, and nuclear spectrum presents a significant challenge. The DSB focused on two of the most dangerous threats: biological warfare and nuclear dispersal devices.

Within DoD, current biodefense technology-development efforts are heavily weighted toward early detection, which is crucial to minimize fatalities and assure continuity of essential DoD capabilities. However, the DSB recommends rebalancing the DoD (and national) research and development investment to better address the effects of a biological attack, by increasing the emphasis on therapeutics, diagnostics, and remediation relative to the current focus on detector technology.

Current technical capabilities for detecting radiological dispersal devices – or “dirty bombs” – are limited, and passive portal detection alone is insufficient to counter the threats of greatest concern. What is needed is an end-to-end concept of operations that would produce a layered and integrated prevention and protection strategy. The key to such a concept is to extend the first line of defense beyond the territorial borders of the homeland. The development of radiation countermeasures for humans should also be accelerated; funding for the Armed Forces Radiobiology Research Institute should be increased significantly to perform this research.

Benefit would come from some centralization of responsibility over the many dispersed programs addressing the CBRNE challenge. The DSB recommends that NORTHCOM be assigned responsibility for setting *requirements* for CBRNE defense of CONUS bases.

Medical Surge. A robust capability for DoD to surge medical treatment is critical but lacking. DoD should significantly expand its capabilities for medical surge to ensure that attacks from weapons of

mass destruction do not compromise DoD's ability to project and protect forces. The Department needs quantitative, end-to-end plans for medical surge for its own forces—a capability that would include providing treatment at bases and critical ports of departure. Realistic reference scenarios would help in the development of such plans.

Despite a focus on protecting military assets, the DoD plan for base installation protection and incident management must recognize that its activities will extend “beyond the fence.” Therefore, medical surge plans must involve coordination with local and state civilian authorities. All medical surge plans should be validated by gaming, red teaming, and realistic exercises.

Communications Operability. More effective communication tools are needed to enable interoperable command and control within the civilian sector and between the civilian sector and the Department of Defense, when its assistance is needed. NORTHCOM and the National Guard, in cooperation with the Department of Homeland Security, have a major role to play in establishing effective operability standards and in deploying critical assets.

Reserve Components. The Reserve Components have vital contributions to make to homeland defense and security and are taking the initiative to enhance their capabilities. The DSB supports these initiatives and recommends additional steps to strengthen their capabilities.

The National Guard is expanding its civil support teams to all 54 states and territories. The DSB encourages extending this state structure to regional units, incorporating a broader set of capabilities similar to those now found in the U.S. Marine Corps Chemical Biological Incident Response Force. The DSB also recommends that the Standing Joint Headquarters being established in each state and territory have strong operational and planning ties to U.S. Northern Command.

One concern of the DSB is that the richness of the Reserve Components today and their relationship to the first responder communities in the states and territories is not well understood. The

individual Reserve Components need to compile and keep up-to-date a complete database of skills and facilities, to be used as a resource in operations and planning. U.S. Northern Command should have access to such a database, as should the adjutants general and state Standing Joint Headquarters. Finally, the DSB suggests the creation and operation, under NORTHCOM, of a Joint CONUS Communications Support Element, using the National Guard.

EXPORTING DOD CORE COMPETENCIES

The recommendations summarized thus far require DoD to work closely with other government agencies in order to meet its own responsibilities in homeland defense and support to civil authorities. DoD can also enhance homeland security by “exporting” relevant core competencies that match the needs of other organizations that have homeland security responsibilities.

The Office of the Assistant Secretary of Defense for Homeland Defense, the U.S. Northern Command and the Department of Homeland Security are all new organizational entities with important roles to play in protecting the homeland. The magnitude of the homeland protection challenge calls for a rapid maturation of their capabilities and establishment of working relationships among them free of the too-common bureaucratic barriers.

The DSB identifies three core competencies in particular:

- Training is perhaps the most important factor distinguishing the capabilities of the U.S. military from those of other nations. Training, and its complementary exercises, provides real-time feedback and hardheaded assessment—fostering adaptability rather than rote learning.
- DoD’s experience with experimentation would be valuable to other organizations. Experimentation could help organizations to explore new operational concepts, identify risks, and guide investment decisions. DoD should work closely

with other agencies as it designs its own homeland-defense and security-related experimentation.

- Operational-level planning and execution is an inherently joint activity for warfighting. More operationally oriented approaches, such as the “joint task force” approach, could be usefully employed by the Department of Homeland Security in fulfilling its responsibilities.

The DSB recommends that U.S. Northern Command (with strong support from U.S. Joint Forces Command) be assigned responsibility to develop, and oversee execution of, plans to export core competencies to DHS and other agencies. U.S. Northern Command should also be tasked to identify ways to apply DoD’s joint-task-force approach to the homeland security challenge. The joint interagency task forces provide a role model.

AN EVOLVING ROLE FOR NORTHCOM

As directed by the terms of reference, the DSB’s study focused specifically on NORTHCOM’s role. In this report, the DSB has recommended fifteen new tasks for NORTHCOM. Requiring the organization to begin execution of all of these new tasks now is not feasible. Priorities are needed, and are addressed below. *The main message, however, is that NORTHCOM must be empowered for the nation to achieve its homeland security and homeland defense goals.*

The DSB recommends that the following four tasks be assigned to NORTHCOM now, along with appropriate authorities and resources

- Develop roadmap for maritime surveillance
- Develop roadmap for defense against the low-altitude air threat
- Assume operational lead for DoD mission-critical infrastructure protection in CONUS (taking on the role of the joint rear area coordinators for the regional combatant commands working with U.S.

Strategic Command and the other combatant commands)

- Assume the lead for exercises, training, experiments, and standards related to homeland defense and military assistance to civil authorities

As stated previously, the DSB envisions a holistic, institutionalized approach to homeland security and homeland defense for the Department of Defense. By taking this approach, DoD should be able to focus on engaging the threat away from the U.S. homeland. At home, its ability to collaborate and communicate with the diversity of players that contribute to the nation's security should be greatly enhanced. In the end, by achieving the capabilities described in the six areas above, the nation can turn a "yellow-orange" homeland security condition into one that is "blue-green."

CHAPTER 1. INTRODUCTION

Homeland security is a top national priority. Developing an effective homeland security capability will involve the direct participation of many federal, state, and local agencies. The Department of Defense (DoD) will be a key player, along with the newly established Department of Homeland Security. Sorting through the roles and responsibilities of the various players is a process that will evolve over the months and years ahead.

What is clear today, however, is that the Department of Defense has a great deal to contribute to homeland security beyond its historic missions of homeland defense and military assistance to civil authorities. Contributions the Department can make include engineering and technical capabilities, technology, logistics expertise, and modeling and simulation capabilities, for example.

As the nation develops a new strategy for securing the homeland, it provides an opportunity for the Department of Defense to evaluate its own role in homeland security and to determine how best to accomplish this mission.

SCOPE

At the request of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD[AT&L]), the Defense Science Board (DSB) formed a task force to address DoD's roles and missions in homeland security. Specifically, the task force was asked to examine the following areas:¹

¹ The complete terms of reference for the *Defense Science Board 2003 Summer Study on DoD's Roles and Missions in Homeland Security* is in Appendix I. Appendix II lists the task force members and the organization of the study. Appendix III provides a list of briefings presented to the task force.

- **Roles and missions for which DoD will be responsible.** Further, what are the derivative unique operational responsibilities of U.S. Northern Command?
- **Processes and requirements for accomplishing these roles and missions.** Specifically, what are the interagency processes that need to be put in place to support an integrated security strategy, planning function and set of operational capabilities? What are the specific information-sharing requirements among DoD and other government agencies, both federal and non-federal? What refinement is needed of theater-security cooperation methods with Canada and Mexico?
- **Vulnerabilities assessments.** How will force projection issues and responsibilities be addressed in the larger context of homeland security?
- **Goals for DoD support to civil authorities.** What are the roles and responsibilities of U.S. Northern Command and the Reserve Components in support of these goals? What are the implications for the warfighting mission of the National Guard and Reserve?
- **Technologies and systems in which DoD should lead research and development efforts.** What are the classes of technologies and systems, with application for homeland security, that DoD should have the lead in developing?²

STUDY APPROACH

Deterring, preempting, and preventing aggression against the United States will remain a priority for the nation in the global war against terrorism. The strategy in this endeavor is to win the war

² Volume II of this report contains a chapter on research and development for technologies and systems that apply to homeland security.

outside of U.S. borders. Thus, this study examines the actions needed to make it more difficult for potential adversaries to achieve their goals on U.S. soil. Should that strategy fail, however, the study also addresses the actions needed to secure the homeland in the event the United States becomes the battleground.

Many aspects of the global security environment have changed dramatically in recent years—and in a way that suggests a new approach to securing the U.S. homeland is needed in the future. Key elements of the security environment that influenced the DSB's approach to this study include the following:

- Operation Enduring Freedom and Operation Iraqi Freedom again demonstrated U.S. conventional military supremacy. This fact, along with terrorist aims to reduce U.S. overseas presence and influence, will drive the nation's enemies to asymmetric attacks, including attacks on the homeland.
- Evidence suggests that weapons of mass destruction—including chemical, biological, radiological, nuclear, and high-explosive (CBRNE) weapons—are in the hands of credible enemies. Deterrence is increasingly difficult to ensure.
- Asymmetric enemies have the capability to conduct a *campaign* against the United States that might include near-simultaneous attacks, attacks that are geographically and/or temporally dispersed, or attacks conducted by insiders.
- The U.S. ability to project force from the continental United States (CONUS) is increasingly at risk.

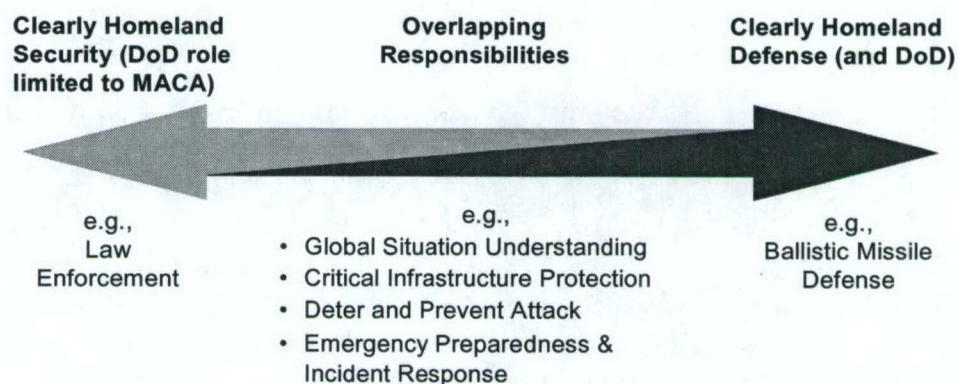
Within this environment, the responsibilities for homeland security will be widespread. DoD's own responsibilities will be to continue in its longstanding roles of defending the homeland against attack, projecting force when directed, and protecting the nation's people and designated critical infrastructure. To meet these responsibilities, however, the Department will need help from others

in several areas: ensuring that non-DoD assets critical to DoD missions are secure and available, and ensuring that information and intelligence critical to DoD missions are available and timely.

In addition, the Department can help others fulfill their responsibilities in homeland security. Opportunities include leveraging DoD's core competencies in training, red teaming, large-scale gaming, and research and development. DoD can also continue its role of providing military assistance to civil authorities and can assist the Department of Homeland Security as it evolves and matures.

Given the complexities of these varied responsibilities, needs and opportunities, the DSB adopted a broad construct within which to assess responsibilities for securing the U.S. homeland – a spectrum that ranges from responsibilities that are clearly homeland security, such as law enforcement, to those that are clearly homeland defense, such as ballistic missile defense. Such an approach will best ensure that the nation is appropriately prepared to respond to aggression against the homeland, but it can also result in overlapping responsibilities between the Departments of Defense and Homeland Security, as figure 1 illustrates. Nevertheless, at this point in time and against today's enemy, the DSB believes that an overlap in responsibilities is far preferable to gaps.

Figure 1. Focus is on Overlapping Responsibilities



The analysis that follows focuses on four areas of overlapping responsibilities judged by the DSB to be near-term priorities for the Department of Defense.³

- Global situation understanding
- Protecting DoD mission-critical infrastructure
- Deterring and preventing attack
- Emergency preparedness and incident response

In addition, the report explores two issues that are cross-cutting in nature, with application to all four areas listed above:

- Exporting DoD core competencies
- Empowering U.S. Northern Command

The chapters that follow discuss each of these areas in turn and offer recommendations for the Department of Defense that will enhance the nation's ability to more effectively secure the homeland in the future.

³ Volume II of this report explores a number of these topics in further detail. Topics covered include information sharing and assurance, technology and systems, emergency preparedness and incident response, and contributions of the Reserve Components.

CHAPTER 2. GLOBAL SITUATION UNDERSTANDING

Today more than ever, information is vital to homeland security. Information is a key to understanding the adversary and to developing an effective awareness of the global security environment. The analysis following the September 11, 2001, attacks focused a great deal on what was known, by whom, and when—in an effort to determine whether more timely disclosure of available information might have prevented the attacks. Consequently, significant effort has been directed to improve the way agencies collect, analyze, share, and protect information.

While some advances have been made in technical capabilities, policy guidance, legal restrictions, and cultural approaches relating to information sharing, much more needs to be done. Improvements are needed in part because the culture of many organizations still focuses on establishing a “need to share” before disclosing information, thus restricting access. A more useful approach today is a construct that promotes sharing information while simultaneously protecting it. Of course information sharing depends on *having* information; thus collection is a critical element in the equation.

The DSB identified two areas where opportunities for improvements exist and progress is essential:

- Enhancing information sharing while improving the ability to assure information integrity, confidentiality, and availability
- Improving the acquisition and analysis of needed information by creating a potent HUMINT capability and by making greater use of open-source information

SHARE AND ASSURE INFORMATION

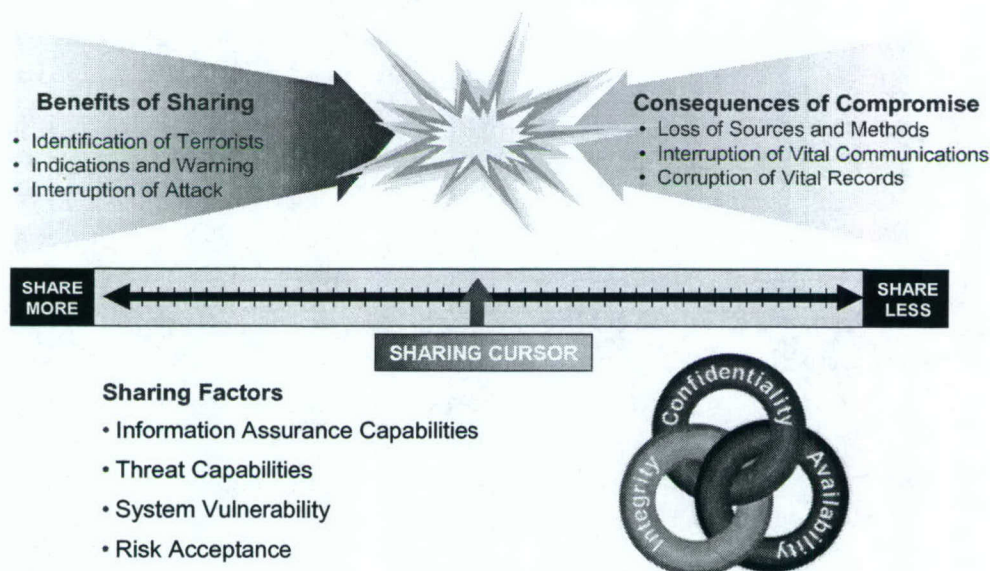
The ability to share and protect information, and to do so in a timely manner, presents a unique challenge to the nation. This challenge is unique because information-sharing and information-assurance requirements extend to a more diverse and dispersed group of individuals than ever before — encompassing federal government agencies, state and local governments, first responders, and the private sector. Thus, converting data into information that creates a common understanding of the homeland security environment — particularly in the event of a crisis — is no small task and will require changes in policy, technology, and organizational culture.

Though the need for information sharing is widely acknowledged, less obvious is the fact that it is also a double-edged sword, as illustrated in figure 2. Greater connectivity between organizations allows increased ease of sharing, which in turn can help identify terrorists, provide better indications and warning, and potentially interrupt intended attacks. However, increased aggregation of data and applications, globally dispersed nodes, and technically complex systems, components, and architectures provide opportunities for an adversary to attack the confidentiality, integrity, and availability of information. The consequences of such an attack could mean a loss of sources and methods, interruption of vital communications, or even corruption of vital records.

Both the benefits and consequences of sharing information must be considered in determining how much information should be shared and with whom. It is critical to effectively manage the risks of information sharing by enhancing the nation's information-assurance posture while implementing new information architectures and technologies. The advances in information technology over the past few decades, and the availability of such technology in the hands of potential adversaries, mean the probability of successful targeting and exploitation of critical information systems is on the rise. In essence, the cyber threat is diverse and growing. Thus, as the value

of information sharing increases, more resources must be invested in safeguarding critical information.

Figure 2. Information Sharing is a Double-Edged Sword



Information Sharing

Information sharing depends on a well-crafted security and assurance policy and sound technology architecture. To achieve such an end state, the Department of Defense should work with the Department of Homeland Security (DHS) and the Department of Justice to arrive at a single coherent—or at least convergent—security policy and architecture that includes personnel security policies and practices and supporting information technologies.

Security Policy

The Departments of Homeland Security and Justice, along with the intelligence community, have taken steps in the direction of creating a common policy for information sharing. In March 2003, the Director of Central Intelligence, the Secretary of Homeland

Security, and the Attorney General, signed a memorandum of understanding (MOU) outlining requirements and procedures that

- Require sharing of information, even under circumstances where the Department of Homeland Security did not request it, or know to request it
- Allow masking of sources and methods as long as substance is not affected
- Demand a responsive (24 hours) declassification or release upon request

The DoD was not a signatory to this MOU. However, the DSB believes that the Secretary of Defense should issue guidance to the Department to abide by the letter and the spirit of the MOU. This step would apply to the entire repository of information available to DoD, not just to traditionally shared intelligence. However, DoD should take precautions similar to masking sources and methods to minimize potential damage in the event of disclosure. DoD should be involved for several reasons.

- DoD has information other than traditional foreign intelligence that is essential for others engaged in homeland security
- DoD requires information from others, such as providers of domestic intelligence, in order to execute its homeland defense and homeland security responsibilities

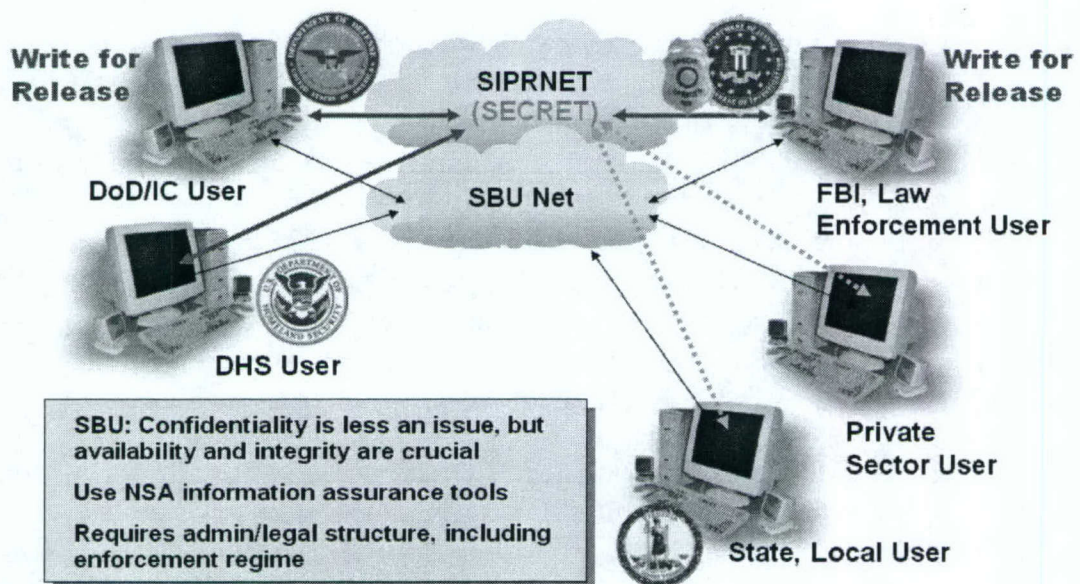
This MOU is a significant step in encouraging sharing, but much work still needs to be done in order to provide the level of sharing and assurance that will be required to meet homeland security needs, as described in the remainder of this chapter.

Information Architecture

Because of the diverse community needing access to homeland security information, it will be challenging to develop a truly coherent information-network architecture. Thus, the architecture

needed should be created with a broad view of the "network," including not just links, but the associated nodes, the relevant human subscribers, the necessary information, and the associated value-added processing. The goal for such an architecture is not simply to share information, but to *share knowledge* in order to jointly achieve common goals that are unattainable by individuals or single departments or agencies. Figure 3 illustrates a concept of operations for a near-term information-sharing architecture.

Figure 3. A Concept for an Information-Sharing Architecture



A single entity, such as an Executive Agent, should be made accountable for development of such an architecture. Having one point of accountability will facilitate development of the required administrative and legal structures, including an enforcement regime. In addition, a new class of information is needed, the development of which involves reconsidering the traditional national security classification approach.

The DSB supports the development of a class of data termed sensitive but unclassified (SBU), which has been referred to by the President and, through executive order, placed under the aegis of the

Secretary of Homeland Security. SBU data would be available to a wider range of communities than traditionally classified national-security and intelligence information. The users of SBU data might include DoD, the intelligence community, DHS, the law enforcement community, state and local users, and the private sector. As appropriate, these individuals would be able to access SBU information through a new network – “SBU-Net.” As illustrated in figure 3, all individuals, connected to the network with appropriate authentication, would have access to the SBU information with a minimum of prior vetting.

According to currently approved divisions of authority, the Homeland Security SBU-Net would be managed from the Office of the Secretary of Homeland Security. However, DoD has considerable capability and expertise in designing, developing, and operating such networks and should make that expertise available to DHS. This expertise, accompanied by investments in future technologies, could well serve DHS and could be provided through DoD in the role of executive agent. Even if this approach is not taken, DoD can play a considerable role in helping formulate overarching policies and architecture for an SBU-Net.

Though the information carried on the SBU-Net may deserve the protection that it would receive in a DoD network such as SIPRNET (Secret Internet Protocol Router Network), it should remain separate. Allowing the larger population of homeland security subscribers access to DoD operational and intelligence information is not desirable. DoD and the intelligence community should operate on (at least) two tiers, handling classified national security information on SIPRNET (or the Joint Worldwide Intelligence Communications System) and preparing other materials especially for release via the SBU-Net, as the concept in figure 3 illustrates.

As the information-sharing MOU calls for, a “tear line” would appear on classified reports where sensitive and classified information is “above the line” while the essentials for action are below the line. Agencies who own reports containing highly classified and sensitive information would create tear-line reports written for use on both tiers of the network. This approach permits a

trusted interlocutor to “tear at the line” and disseminate appropriate information further – via the SBU Net – to a set of less vetted subscribers than receive classified information.

In addition to investing in infrastructure and data bases, agency leaders must also address the many barriers to information sharing – barriers such as a lack of knowledge about the value of information, cultural impediments that place more value on “keeping” than “sharing” information, weak data infrastructures, and statutory or regulatory constraints. To reduce such barriers, it is necessary to put into place positive, tangible incentives to reinforce information sharing. For example, incentives might reward information “stewards” not only for effective collection, protection and storage of information, but also for its widespread use. Leaders across government must assess their individual organizations to determine if the right incentives are in place to promote the kind of information sharing that is desirable.

An Information-Sharing Laboratory

In pursuit of more effective and expansive information sharing, the DSB recommends that an advanced concept technology development (ACTD) program be initiated to create a laboratory that is capable of testing evolving policies, tools, and techniques for information sharing. The laboratory would be a place where new approaches for information sharing, classification, data tagging, and collaboration could be tested as well.

The DSB recognizes that there is not likely to be a single network for homeland-security information sharing; rather there will be many networks that operate together to transfer information among users. Thus, the laboratory would function as an “information roundhouse” where many disparate networks could be brought together in one operational space – in fact one physical space – to conduct realistic interoperability experiments. The laboratory would be used in all homeland security exercises and be instrumented so that meaningful metrics could be produced from the exercise scenarios.

Because U.S. Northern Command (NORTHCOM) has a homeland defense mission that will require deep and continuing interaction and information sharing with DHS and other agencies, it is both a logical sponsor for the ACTD as well as a logical location at which to host such a laboratory. After the program is established, NORTHCOM would be in an ideal position to oversee expansion of the ACTD, as appropriate, to other DoD networks such as the SAFECOM program, described in chapter 5, and the Joint Tactical Radio System. Analyses and results from the ACTD should be shared with the Departments of Homeland Security and Justice. An information-sharing laboratory can be used government-wide to test and assess improvements in the nation's ability to share and assure homeland security information.

Information Assurance

Today the technical shortcomings of information assurance are significant, and the gaps are increasing. As the advantages to the adversary continue to increase and the nation's defensive capabilities decrease relative to those advantages, improvements must be made in the national information-assurance capabilities. These improvements include developing better techniques for discovering system weaknesses, designing effective defenses, and developing consistent metrics for the impact of compromise to systems. Improving information assurance also means paying more attention to information integrity and availability, in addition to confidentiality issues.

Increased Capability Means Increased Vulnerability

The advances in complexity, affordability, and performance of information technology over the past 20 years have made the United States more dependent than ever on computer systems and applications performing a myriad of daily tasks—in banking, commerce, power generation and distribution, medical services and records, physical security, telecommunications, nuclear weapon command and control, taxes, inventory control, social benefits, and countless other areas.

In addition, a growing percentage of software is being designed, coded, distributed, and maintained overseas. Consequently, U.S. adversaries could have unprecedented direct and indirect operational access to many of the nation's most vital systems. Coupling this advantage with the fact that much of the U.S. microelectronic fabrication is being done offshore, the clever adversary has the opportunity to own key systems in a deeply concealed manner.

With both the capability and complexity of hardware- and software-based components increasing at the rate of Moore's Law, the ability to detect anomalies, control configuration, and evaluate and assure the trustworthiness of these systems is markedly diminished. A classified experiment conducted in the mid-1980s demonstrated the overwhelming challenges of discovering subversive constructs in microcontroller-based systems of the time. The complexity and dynamics of today's technology makes the ability to perform credible vulnerability assessments even more challenging now, if not impossible.

Advances in microtechnologies not only benefit the United States, they also create the opportunity for adversaries to attack the United States in unconventional ways. Today, the United States has no adversary or opponent that can successfully engage in a conflict using conventional strategies. Thus adversaries will turn to asymmetric or unconventional approaches to attack the United States – with attacks to critical information-technology infrastructures being one such approach.

Ironically, the Blaster worm hit many computers across the country, including those used by the members of the DSB, during the deliberations of this study. While cleverly implemented, this worm and the techniques used to launch it are simple compared to the capabilities of sophisticated opponents. Yet even with a modest level of technology and tradecraft, a hacker was able to wreak havoc with even some of the most capable of defenses in the United States. A capable adversary can be successful in exploiting U.S. systems, which means that considerable resources must be devoted to countering this threat.

Addressing Vulnerabilities

Only one organization in the country has the culture, expertise and critical mass to take the lead in addressing these information vulnerability challenges – the National Security Agency (NSA). The NSA Information Assurance Directorate (IAD) has the largest and most experienced group of information-assurance experts in the country. While there are areas within IAD that require considerable improvement, it is the only large cadre of information-assurance professionals that enjoy close organizational proximity to the NSA signals intelligence directorate and its expertise. Although collaboration between these two groups could increase, the relationship that already exists has enabled a group of IAD professionals to develop a clear understanding of how the offensive game is played with respect to information. This understanding is essential to enable defenders of information systems to invest resources, develop defensive barriers, promote strategies, and establish policy that will be effective in countering adversary capabilities to compromise U.S. systems.

The nation is both vulnerable and a target that could be exploited in an undetected fashion by sophisticated adversaries. The conundrum is that the United States must take advantage of information systems in order to stay at the leading edge and be effective in combating terrorism. At the same time, the risk of exploitation by adversaries increases. This situation requires that the nation adopt a strategy for managing the increasing risk, which is easier said than done. In order to develop and maintain an effective risk management program, the United States must know what needs to be kept secret and thus requires added protection; know its adversaries, their capabilities, limitations, constraints, resources, and partners; identify vulnerabilities; and, finally, understand defensive options.

There are positive steps that can be taken now to offset the current advantages of the adversary and work towards an effective risk management strategy. These steps include the following:

- Significantly increase collection requirements, analysis, and reporting on foreign information operations capabilities, organizations, players, and partners.
- Share this growing body of insight with those responsible for National Information Assurance policy and solutions.
- Task the National Security Agency's Information Assurance Directorate with the authority and responsibility for all aspects of information assurance as it relates to homeland security. Provide NSA with the necessary resources.
- Institute a threat-reduction investment strategy. All research, technology investments, and production should be directly tied to decreasing the advantage of opponents.
- Identify data and applications where the benefit of sharing is minimal and the consequence of compromise (confidentiality, integrity, or availability) is unacceptable, and provide appropriate technical and procedural measures to ensure isolation. Nuclear command and control is an example of such an application.
- Identify nodes where a single point of failure results in dramatic consequence and minimize the application of foreign software and hardware in these nodes. Where foreign components must be utilized, the most rigorous security evaluations must be conducted.
- Develop risk management processes that balance: threat technical/operational capabilities, defensive measures in place, vulnerabilities, operational risk to the adversary, technical and operational cost to the adversary, costs of technical and procedural measures that can offset adversary advantage, and impact of a successful adversary operation.

- Educate senior decision makers on this process and its associated elements.
- Task the National Research Council to assess the current status of U.S. information-assurance research and its associated impact on mitigating the threat.
- Commission a national study to examine, in depth, the information-assurance issues identified in this report.

RECOMMENDATIONS

SHARE AND ASSURE INFORMATION

The Secretary of Defense should sign the March MOU on information sharing that was signed by the Director of Central Intelligence, the Secretary of Homeland Security, and the Attorney General

- Directs DoD participation
- Allows masking of sources and methods as long as substance is not affected—requires “tear-line” reporting
- Supports “sensitive but unclassified” information-sharing mechanism

Conduct risk assessments to balance benefits of sharing with consequences of compromise

Task NSA as the exclusive provider of information-assurance policies and solutions for DoD and DHS networks

Fund the NORTHCOM ACTD on information sharing

IMPROVE INFORMATION COLLECTION AND ANALYSIS

To benefit from improved information sharing and assurance, there must be information of value to share. Much has been done over the past decade to improve foreign intelligence collection, beginning with efforts made during Operation Desert Storm and

continuing through Operation Enduring Freedom and Operation Iraqi Freedom.⁴ However, further improvements are needed in intelligence collection as well as information integration and analysis to meet the added requirements of homeland security.

Foreign Intelligence Collection

A recent DSB report, not yet published, offers many recommendations for improving the posture of the foreign intelligence community to more deeply penetrate terrorist threats, recommendations that the DSB endorses. That study emphasized concepts for making intelligence collection more proactive and provocative. This means the intelligence community must transform from a culture of simply "gathering" information as it becomes available to one of actively "hunting" for information that supports a particular need.

The community must pay more attention to "target development," involving collectors, technologists, and operators to improve the depth and quality of analysis. Gaps in foreign-language capabilities and cultural and technical skills must be closed. The intelligence community also needs to improve "horizontal integration" of intelligence collection disciplines so that information is better integrated between the traditional disciplines. Greater use of red teaming, modeling, and simulation can also be made in the area of foreign intelligence.

Finally, the partnerships that exist between government and industry are critical to successfully transforming DoD and the intelligence community so they may more effectively deal with the terrorism threat. This transformation will require defining new ways of doing business, maximum use of special authorities (held by the Director, Central Intelligence) for streamlined acquisition, and reinvigorated collaboration for collection, analysis, and information access.

⁴ This issue has been the topic of several Defense Science Board studies.

A Robust Human Intelligence Capability

DoD must also establish a more robust Defense human intelligence (HUMINT) capability than exists today. The Defense HUMINT Service must be reinvented to provide improved battlefield support and augmented collection. This reinvention requires improvements in both human-derived and technical capabilities. A more effective HUMINT capability requires an elite force of specialized people and capabilities, and the nature and character of their operations and technical access means must be improved and kept secure. New initiatives are needed to improve overall battlefield intelligence, surveillance, and reconnaissance (ISR) in areas such as improved dwell time, pervasiveness, penetration, survivability, and stealth.

Information Integration and Analysis

Domestically derived intelligence and foreign intelligence need to be more effectively integrated to ensure homeland security. The Terrorism Threat Integration Center (TTIC) for warning and analysis was established for just this purpose. The challenge for the TTIC will be to bring together the sources, methods, and cultures of the defense, law enforcement, homeland security, and intelligence communities to create an information and reporting environment that shares, correlates, and directs all sources of terrorism threat information.

Of additional importance is the continued development of collection and target-access means that expose and define terrorism threats, both foreign and domestic. One of the highest-leverage ways to improve this capability is through a rigorous, disciplined process of continuous target development. Only with a tight coupling between collection and analysis, and between foreign and domestic intelligence processes, will the nation be able to improve its ability to successfully counter the terrorist threat.

Major upgrades are needed in all areas of intelligence collection—in signals, imagery, measurement, and signature intelligence, for example—and more use must be made of open-source collection.

Critical to the success of such upgrades would be unprecedented integration between the analysis and collection parts of the process. The analytic component of intelligence needs to be more highly interactive with collection. In addition, both general-purpose and specialized analysts in all disciplines need to be physically or collaboratively collocated to create the maximum degree of target development and focus. New organizational, process, doctrinal and collaboration approaches and methods are needed to create a more horizontally integrated community and to ensure that security is maintained while facilitating maximum information sharing.

There are many areas where sharing can be expanded between the foreign and domestic intelligence communities; more can be shared than just analysis and information. These areas include technology for penetrating targets; tools, techniques, and methodologies for the effective conduct of HUMINT; effective means for analysis; sanitization processes and multi-level security technology for protecting sources and methods; and effective technologies and processes for reporting, database management, and client access. In order to ensure standardization and interoperability, the intelligence community can share communication architectures, technologies for bandwidth extension, information-assurance technologies and approaches, and even warfare byproducts related to information warfare and information operations.

The ultimate key to more effective information integration and analysis is communications and collaboration. Major steps need to be taken to maximize initiatives that make quantum improvements in these areas, including physical collocation, cross-detailing of personnel, and resource and technical investment in collaborative tools that facilitate secure dialogue at appropriate levels on problems of mutual and critical interest.

RECOMMENDATIONS

IMPROVE INFORMATION COLLECTION AND ANALYSIS

Improve foreign intelligence capabilities by employing new/adapted HUMINT modes of operation that

- Penetrate into global “badlands” and other sanctuaries
- Employ cyber tradecraft
- Specialize in clandestine-technical activities

Enhance collaboration between DoD and DHS in systems engineering, architecture skills, technologies, and methodologies to improve integration of domestic and foreign intelligence. Approaches include:

- Network-centric architectures
 - Advanced analytic processes, procedures, and tools
 - Innovative strategies for integrating intelligence
-

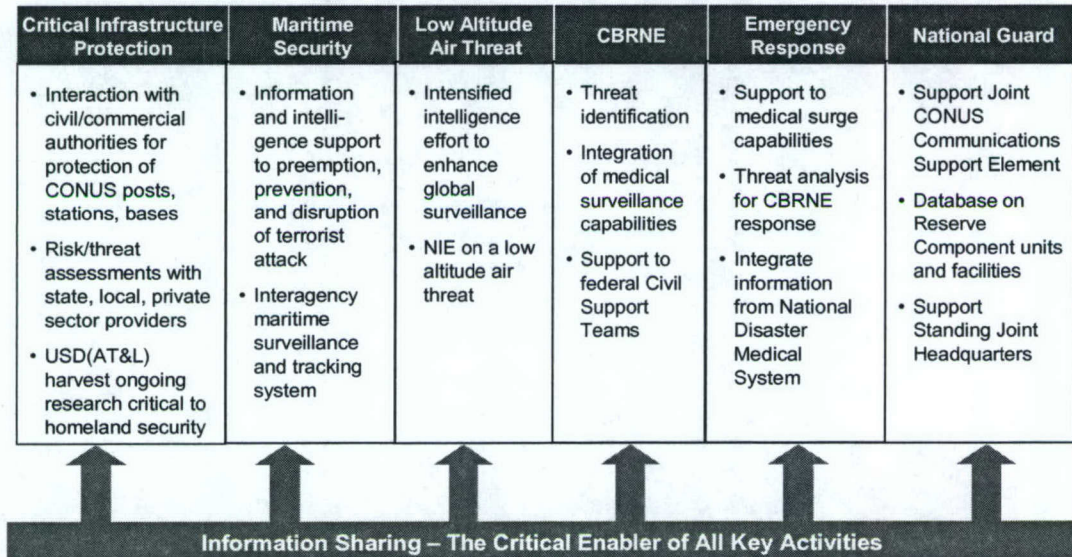
INFORMATION: A CRITICAL ENABLER

As this chapter has portrayed, creating global situation understanding requires far more of the U.S. government than simply increasing the flow of information between and among agencies. New information-sharing architecture and policy must be developed to ensure that a common operating picture can be created for all those involved in homeland security concerns. More effective information sharing will require better foreign intelligence collection, better collaboration among domestic and foreign intelligence agencies, and, in many cases, cultural change as well. These changes are not simple to implement, but they are necessary steps to improving homeland security.

Global situation understanding is not an end in itself. It has an impact on all aspects of homeland security, as will be discussed in the following chapters of this report and is illustrated in figure 4. Thus,

the integrity, confidentiality, and availability of homeland security information require continued attention and action.

Figure 4. Information Sharing is a Critical Enabler



CHAPTER 3. PROTECT DoD MISSION-CRITICAL INFRASTRUCTURE

DoD's ability to fulfill its missions – most notably force projection – is dependent on an intricate infrastructure in the United States. The majority of this infrastructure is not owned or controlled by DoD or the federal government, but by the private sector or state and local governments. DoD mission-critical infrastructure encompasses many diverse parts: military bases, transportation, communication, power, fuel, food, ammunition, other logistics, and the defense industrial base. Both physical and cyber attacks on this infrastructure are of concern and there is potential for "single-point failures."

Adversaries may have increasing incentive to target mission-critical infrastructure as well as DoD personnel and their dependents. Incentives include the following:

- Military: don't let U.S. military forces into our neighborhood otherwise we lose
- Strategic: attacking targets in the United States shows we have global reach
- Revenge: the U.S. military attacked our families, we will return the favor by killing members of their families
- Political "sensitivity": attacking military targets instead of civilians directly may have appeal to some (not all or even most) adversaries in order to influence world opinion

CRITICAL CHALLENGES LIE "OUTSIDE THE FENCE"

While some good work is being done to address the critical infrastructure problem, overall DoD is not doing nearly enough to respond to the vulnerabilities of mission-critical infrastructure and services, particularly in areas outside of its direct control – "outside the fence."

The DSB appreciates that distributed authorities and ownership of mission-critical infrastructure present challenges for DoD. The DoD ideal—clear responsibilities and authorities—is difficult to achieve with regard to this challenge. The DSB is concerned that consequently there are not enough people in DoD staying awake at night worrying about the problem.

The DSB notes two common reactions within DoD to the term “DoD mission-critical infrastructure.” One is that only the noun “infrastructure” is heard, and the modifier “DoD mission-critical” is ignored. This interpretation leads to the attitude that infrastructure protection is not a DoD responsibility. Alternatively, infrastructure protection is sometimes interpreted to refer solely to *site* protection and to the question of specifically who is responsible. Both perspectives ignore the larger challenge of taking a *comprehensive, systemic view* of the mission-critical infrastructure, which includes people, dependents, and irreplaceable civil resources “outside the fence.” Neither view acknowledges the size of the challenge or its import to the Department. The DoD cannot wait for other government agencies to take the initiative regarding DoD mission-critical infrastructure. Nor can DoD believe its responsibilities stop at the base fence.

DoD mission critical infrastructure protection must be addressed in the terrorists’ “operational trade space” which does not correspond to U.S. government organizational boundaries. DoD mission-critical infrastructure protection

- Is not the same as force protection
- Is more than base protection
- Is not just things ... it’s people and functions ... on and off base
- Encompasses privately owned elements that are often more vulnerable than a base itself

Protection of the critical infrastructure for DoD force projection and sustainment requires a focus on more than a thousand individual assets—some under the command or control of the individual

services, others under the control of one of the various DoD agencies, still others under the many states' adjutants general. One compilation of DoD mission -critical assets, organized by the Joint Program Office-Special Technical Countermeasures (JPO-STC), estimates that over 75 percent of these assets are in the private sector. Further, many assets—energy, telecommunications, water, transportation, and fuel networks—are often more susceptible to a single point of failure from disruption of the local supporting commercial infrastructure than from physical destruction from kinetic or other cyber attacks aimed at the site itself.

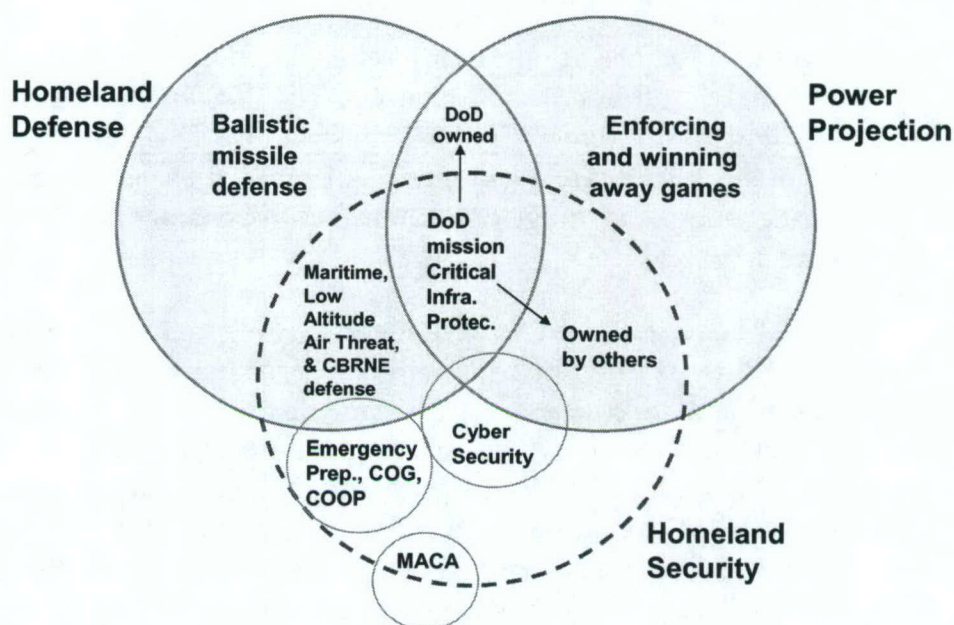
These supporting private-sector infrastructure entities are governed by a plethora of regulatory schemes, insulating them from the traditional requirements and leverage that the DoD has over its suppliers. Furthermore, within this infrastructure, DoD sites (installations, etc.) are rarely purchasers of sufficient scale to have significant economic leverage over their non-governmental "providers."

Because it does not own or have leverage over many of the assets it needs to fulfill its mission, DoD will need assistance from other agencies and private entities in addressing its own mission-critical infrastructure challenge. Thus, addressing the protection of mission-critical infrastructure will require both enlightened leadership and "followership" on the part of DoD. The next section of this chapter describes some existing collaborative approaches that could help DoD in formulating appropriate policy solutions to infrastructure protection.

The DoD policy solutions for total critical infrastructure protection, including protection of the defense industrial base, should seamlessly connect with the DHS promulgated guidance and rule-sets for privately owned and operated supporting infrastructures. The national and regional policy for these infrastructure intersections should then be reflected in the specific plans developed to protect sites and bases and implemented by the various services, agencies, and state National Guard headquarters.

Figure 5 illustrates three complementary responsibilities: DoD's force projection, DoD's homeland defense, and DHS's homeland security. Highlighted are several missions for which DoD and DHS must work together. In addition to critical infrastructure protection, these missions include dealing with the maritime, low-altitude air, and CBRNE threats, which are addressed in subsequent chapters of this report.

Figure 5. Critical Infrastructure Impacts Homeland Defense, Power Projection, and Homeland Security



CURRENT ACTIVITIES

There are activities underway in DoD that can serve as models for an expanded critical infrastructure protection effort. The DSB highlights two of these: U.S. Pacific Command's (USPACOMs) war plan, tied to mission-critical infrastructure, and the U.S. Marine Corps' work with the local community around Camp Lejeune, North Carolina. It is important, however, to note that even these "best-in-class" examples focus more on the security of "things" and do not

sufficiently address the challenge “outside the fence” — such as people or warfighters’ dependents off base — which leaves a significant vulnerability unaddressed. Future efforts, which can draw on the experiences described here, must also take the broader view of mission-critical infrastructure protection recommended in this report.

The USPACOM Experience

Exercises and red teaming helped identify vulnerabilities to critical infrastructure. PACOM played an extended theater of operations in the Ulchi Focus 99 exercise and the red team exploited the extended theater by attacking targets in Guam, Hawaii, and CONUS to thwart deployment of U.S. forces.

The involvement of PACOM’s senior leadership was necessary to ensure follow-up of exercise results and assign responsibilities. For example, Commander, PACOM, established several flag-rank joint rear area coordinators (JRACs) within PACOM (eventually in Hawaii, Guam, Alaska, and Japan) to deal with the identified challenge. Subsequent exercises explored ways to address the problem.

Resources were made available to support analysis and experiments: critical infrastructure protection funds from the Office of the Secretary of Defense (OSD) were used to develop a web-based “deployment picture.” (A little money — a few million dollars — can go a long way in the combatant commands). OSD critical-infrastructure protection funds also paid for support from the JPO-STC to help identify the critical installations and infrastructure supporting a PACOM war plan and conduct analysis and assessments of their vulnerabilities.

As a result of these assessments, PACOM expanded working relationships with both the private sector and federal, state, and local governments in Hawaii, Alaska, and Guam to identify vulnerabilities and solutions for mission-critical infrastructure (DoD-owned and other). This process included frequent exercises (every three months) and heavy involvement of non-DoD participants in these exercises.

Cooperative initiatives such as the Hawaii Emergency Preparedness Executive Committee, the Hawaii Energy Council, and the Joint Armed Services/ State of Hawaii Civil Defense Coordinating Committee have strengthened partnerships valuable not only in terms of training and exercises, but also in establishing information-sharing links and joint solution structures to deal with challenges in the future.

The first Appendix 16 ("Critical Infrastructure Protection") to a commandant commander's operational plan was prepared. This appendix contains instructions and policy guidance for critical asset identification, vulnerability analysis, and identification of remedial options.

New tools and capabilities were developed to facilitate cooperation with state and local agencies. These include the Area Security Operations Command and Control (ASOCC)—an interactive computer-based system to provide situational awareness to commanders and collaborative planning capabilities for use with civil authorities. PACOM and the island's civil authorities have collaborated in establishing a specialized communications interface (Pacific Mobile Emergency Radio System) that allows for direct transmissions between the military and the island's first responders.

PACOM also established a joint intelligence support element available 24-hours-a-day and a counterintelligence and law-enforcement coordination cell. These initiatives and resultant capabilities not only provide for protection of military installations and protection of key DoD facilities and critical infrastructure, but also for coordination for military support to civilian consequence-management activities in the event of a natural or man-made disaster.

The U.S. Marine Corps Camp Lejeune Experience

The Military-Civilian Task Force for Emergency Response (MCTFER), a partnership between the U.S. Marine Corps Camp Lejeune and the city of Jacksonville, North Carolina, is another example of cooperative, complementary efforts between military and non-military entities. While not yet focused on infrastructure

protection, it exhibits the type of military, local, and state government cooperation that will be needed.

The purpose of this partnership is to coordinate all regional emergency services assets (military and civilian) in the event of a disaster in the region (natural or manmade). The partnership operates under an approved incident command system that provides for a unified, coordinated response to a major incident affecting the general welfare of the greater community surrounding Camp Lejeune. The scope is defined in a charter signed by representatives of 12 state and local organizations, including 5 city mayors.

MCTFER's charter builds upon a logical extension of DoD's Directive 3025.1, "Military Support to Civil Authorities," which allows local military commanders to render immediate assistance to civil authorities in order to "save lives, prevent human suffering, or mitigate great property damage under imminently serious conditions." The memorandum of understanding that preceded the group's charter established response criteria for civilian and military emergency service organizations, and follow-on agreements have been used to address liability and policy issues that in the past would have stood as obstacles to efforts such as this one.

In the same spirit as PACOM's initiatives in Hawaii, MCTFER's cooperative efforts have resulted in exercise plans, information sharing, contingency planning, and the periodic establishment of working groups to address problem issues as they emerge. Personal commitment and the pooling of resources have led to a number of innovations and opportunities in Jacksonville and Camp Lejeune, to include creating a mobile incident-command facility for regional response and hosting two Defense Threat Reduction Agency programs, one for unconventional nuclear warfare defense and the other the Joint Service Installation Pilot Program for Chemical and Biological Defense.

THE CYBER THREAT

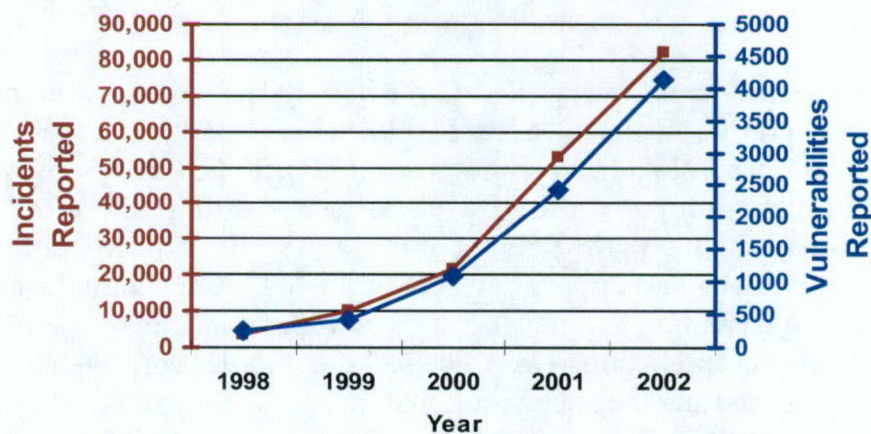
The cyber threat needs to be better integrated into DoD mission-critical infrastructure protection efforts, which have largely focused on physical

attacks. Despite greatly increased investment and awareness over the last five years, information technology and systems remain vulnerable to cyber attacks.

Over the past five years, the number of reported vulnerabilities and incidents on the Internet, the public telephone net, the power grid, and DoD networks has increased, as illustrated in figure 6. The following factors have contributed to this increase:

- An increasing percentage of incidents on DoD NIPRNET are due to “new” intrusion methods.
- Many critical infrastructure information systems (e.g., SCADA systems) are not well protected.
- Trends in broadband network convergence (voice, data, and video) for both industry and government applications create operational value, but also provide more targets and cover for attackers.⁵

Figure 6. Information Technology and Systems are Increasingly Vulnerable to Cyber Attacks



There are ways to improve early-notice (indications and warning) of attacks on DoD-critical networks. Real-time sharing of network and system data would help provide short-term predictive warnings.

⁵ Further discussion of the cyber threat can be found in the *DSB Summer Study on Defensive Information Operations*, 2000.

Many major security incidents have exploited vulnerabilities that have been known (to some) for months.

New tools can help blunt and attribute the source of attacks. Current “signature-based” tools—such as virus software and intrusion-detection systems—are not sufficiently robust. Adaptive, scalable, intelligent security architectures are needed to support a “defense-in-depth,” using network and system back-up and fallback architectures to help in the event of partial failure of defensive measures.

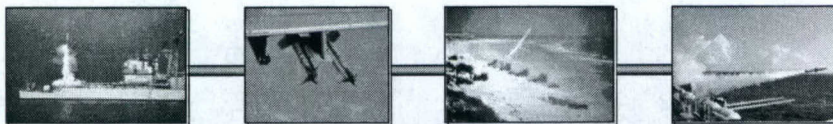
THE DEFENSE INDUSTRIAL BASE

The defense industrial base is another element of the DoD mission-critical infrastructure challenge. The “Tucson story” is an example of the kind of vulnerability that can exist in certain sectors of the defense industrial base. Figure 7 shows the concentration of missiles produced in Raytheon’s manufacturing facilities in Tucson, Arizona. The JTO-STC conducted a vulnerability analysis of this region and identified a number of real concerns that call for improved industrial-base protection measures.

Figure 7. Missiles Produced in Tucson

The following missiles are manufactured in Tucson, Arizona

- | | |
|---|---------------------------|
| • AIM-9X | • Phoenix |
| • AMRAAM | • RAM |
| • EKV (Exo-atmospheric Kill Vehicle for the BMD system) | • Sparrow |
| • ESSM (Evolved Sea Sparrow) | • Standard Missile |
| • Javelin | • Stinger |
| • Maverick | • TOW (anti-tank missile) |
| • Phalanx | • Tomahawk |



All of Raytheon's missiles except Hawk and Patriot (Massachusetts)

WHAT DoD NEEDS TO DO

Integrated vulnerabilities and interdependencies, and the opportunities they present to enemies, reinforce the notion that DoD's concerns regarding anti-terrorism, force protection, information-assurance, continuity of operations, and readiness are community concerns that cannot stop at the installation fence. A concerted, cooperative, and systemic effort must be put forth by the military, and the civil sector it serves, in protecting the assets critical to both. These protective efforts must be free of debilitating organizational boundaries, dysfunctional procedures, and institutional biases — on both sides of the fence.

The DSB recommends that the Secretary of Defense assign responsibilities and authorities to initiate a more comprehensive and sustained effort to identify DoD mission-critical assets, infrastructure, and capabilities and their vulnerabilities. Within the DoD, the policy for the protection of this infrastructure must be driven by a single responsible individual, capable of bridging the civilian-support and military-operational entities. That individual must operate as part of the working policy subgroups under the Homeland Security Council where many of these issues are addressed.

This single point of policy coordination ought to be the Assistant Secretary of Defense for Homeland Defense (ASD[HD]), enabling direct participation in the Homeland Security Council. The ASD(HD) is also positioned to advise the Secretary of Defense, who must issue the necessary directives through the operational and supporting chains of commands.⁶ Through the ASD(HD), the DoD must press its interests in the interagency process for needed external regulatory and financial relief.

The DSB further recommends that the Commander, NORTHCOM, be given responsibility, authorities, and resources to take the lead on implementing many of these infrastructure

⁶ The Secretary of Defense has appointed the ASD(HD) as the responsible office for all DoD critical infrastructure protection activities.

protection initiatives. Specifically, working closely with ASD(HD), the services, and other commands, NORTHCOM would

- Integrate cyber security into critical infrastructure-protection initiatives
- Conduct risk/threat assessments, working with state and local government officials and private sector providers
- Prioritize vulnerabilities based on mission, function, threat, and consequences
- Develop a comprehensive remediation plan working with other federal, state, and local government officials and private-sector providers
- Monitor implementation and assess remediation (including use of red teams)

In fulfilling these tasks, NORTHCOM would serve the role for the regional combatant commanders that the JRAC coordinators do in PACOM.

The overall policies and plans developed by ASD (HD) and NORTHCOM must be reflected in the specific plans developed to protect DoD sites and bases. NORTHCOM would not be responsible for force protection or individual base protection. Its policies would be implemented by the various services and cognizant agencies. The DSB envisions a key role for the National Guard, which is discussed in chapter 5.

To provide the resources that NORTHCOM will need, the DSB recommends that the Joint Program Office-Special Technology Countermeasures be expanded and assigned to NORTHCOM to aid in identifying mission-critical assets, infrastructure, capabilities and vulnerabilities. The functions of this office have evolved over the years, and the Navy special program is no longer an appropriate home for this important joint resource. The JPO-STC should also be tasked to disseminate its methodologies to DHS and others.

Additionally, the DSB recommends that the Secretary of Defense and the Chairman, Joint Chiefs of Staff (CJCS) task USD (AT&L) to address defense-industrial-base vulnerabilities and to devote more research and development (R&D) resources to the following areas: 1) attribution, prediction, modeling, and simulation technology and 2) fundamental improvements to Internet infrastructure protection and remediation of security issues for infrastructure systems, notably SCADA systems. Further, throughout all aspects of critical infrastructure protection, there is a role for the Assistant Secretary of Defense for Legislative Affairs (ASD[LA]) to play in identifying and defining where DoD needs regulatory and legislative relief.

RECOMMENDATIONS

CRITICAL INFRASTRUCTURE PROTECTION

Secretary of Defense should assign the lead policy role for the DoD Critical Infrastructure Program to ASD(HD)

- Establish partnerships and processes with DHS and other agencies

Secretary of Defense and Chairman, Joint Chiefs of Staff should

- Assign NORTHCOM lead responsibility and grant authorities and resources to execute the tasks described above
- Assign the Joint Program Office-Special Technology Countermeasures (JPO-STC) to NORTHCOM; enlarge and fully fund
- Enhance the capabilities of the JPO-STC and task it to disseminate its methodologies to DHS and others
- Task NORTHCOM to work closely with U.S. Strategic Command in cyber security

USD(AT&L) should address the vulnerabilities of the defense industrial base

- The Tucson problem

Invigorate DoD's critical infrastructure protection program

- Operationalize Appendix 16 process at combatant commands
 - Requires a civil/military effort
-

RECOMMENDATIONS
CRITICAL INFRASTRUCTURE PROTECTION (CONTINUED)

Direct USD(AT&L) to devote more R&D resources to

- Attribution, prediction, modeling and simulation technology
- Remediation of security issues for infrastructure systems, notably SCADA systems

Task the ASD(LA) to identify and define where DoD needs regulatory and legislative relief

The cyber-security threat needs to be addressed on a number of fronts. U.S. Strategic Command (STRATCOM) and NORTHCOM should collaborate to form a cyber-security partnership for critical infrastructure protection. In addition, NSA needs to strengthen the National Information Assurance Program certification process for DoD networks, which was discussed in more detail in the previous chapter. This multi-front approach is needed to provide a comprehensive response to this challenge.

RECOMMENDATIONS
CYBER SECURITY

STRATCOM and NORTHCOM need to form an effective cyber security partnership for critical infrastructure protection

DoD should export cyber-security expertise throughout government

NSA should strengthen the National Information Assurance Program certification process for DoD networks

DARPA should focus information technology R&D on fundamental improvements to Internet infrastructure protection

CHAPTER 4. DETER AND PREVENT ATTACK

Deterrence, preemption, prevention, and disruption are priorities in dealing with aggressors against the United States. The preference of the nation is to fight aggressors beyond U.S. borders—to deter, and if necessary defeat, hostile state and non-state actors before they can attack U.S. territory, citizens, or infrastructure. Much effort has been and is being placed on strengthening U.S. capabilities to deter, preempt, prevent, and disrupt. For example, the United States has an overt policy that preemptively acts against states harboring terrorism. Campaign planning is ongoing for the global war on terrorism. And investments are being made to enhance development of a global strike capability.

The DSB supports these ongoing efforts, but chose to address another area where additional focus is needed—that of reducing regional maritime vulnerabilities. Two elements of that challenge are addressed in this report:

- First, improvements are needed in maritime surveillance capabilities. DoD needs to work with the Department of Homeland Security and other civilian departments and agencies to develop a well-integrated, interagency maritime surveillance capability.
- Second, defense against low-altitude air threats must be improved. Cruise missiles and other low-altitude aircraft—especially if armed with biological warfare agents or nuclear devices—are a serious concern.

To effectively implement these improvements and create a more integrated air and maritime defensive perimeter, the DSB recommends establishing a new command—the North American

Defense Command – a concept that is addressed in the final section of this chapter.

EXTEND MARITIME DEFENSE

The ocean borders of the United States create vulnerability to threats from the sea. It is possible for potential adversaries to use commercial vessels to bring a cruise missile or unmanned aerial vehicle within striking distance of U.S. territory or to transport a weapon of mass destruction, possibly in a shipping container, into a U.S. port. Current capabilities to detect these threats and to rapidly mobilize proper assets in response are improving but remain inadequate.

What is needed is a maritime surveillance system that draws on existing capabilities in a seamless manner – fusing national-security, law-enforcement, and commercial information to detect and disrupt possible aggressor actions. A full spectrum of capabilities is available, residing in the intelligence community, the commercial sector, the Departments of Defense and Homeland Security, and other federal agencies. These capabilities include intelligence assets, container security, trade partnerships, tracking, surveillance and reconnaissance, and firepower. Benefits from combining these assets into a maritime surveillance system will be widespread and include improvements in indications and warning, drug interdiction, the cueing and tracking of suspicious cargo and vessels, and assessment of threats approaching the NORTHCOM area of responsibility.

Elements of a Maritime Surveillance System

Figures 8-10 illustrate the various assets that could contribute to an integrated, national maritime surveillance system. The various assets are discussed below, in turn.

Figure 8. Intelligence Community Assets

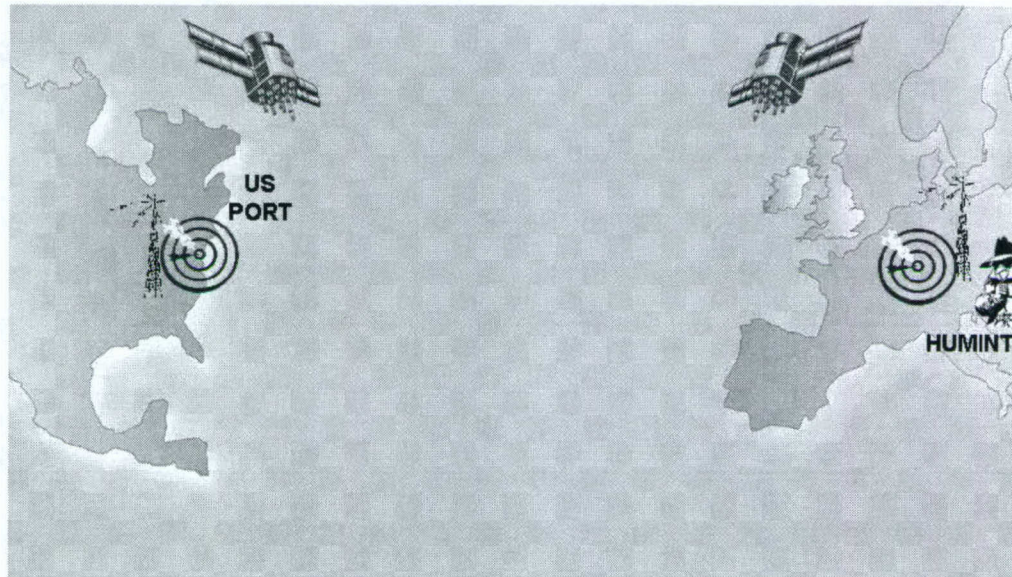


Figure 9. Commercial Data

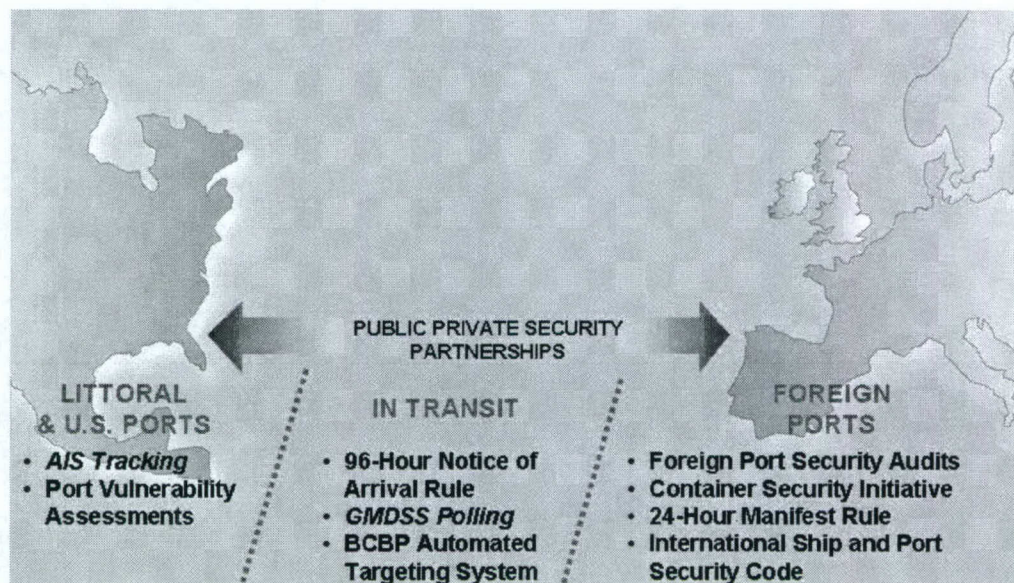


Figure 10. DoD and Coast Guard Capabilities

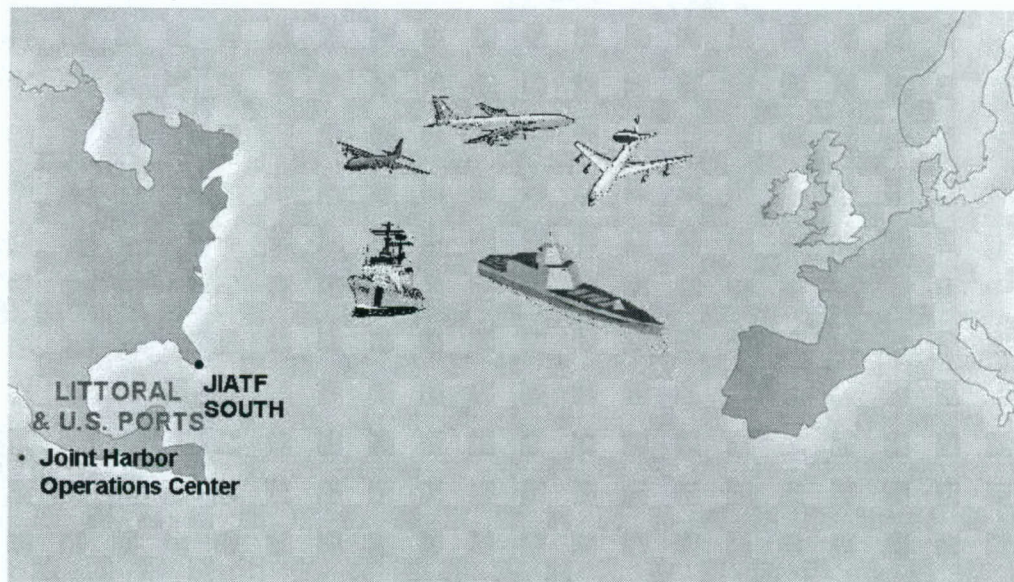


Figure 11. Combined or Federated Maritime Surveillance System



Intelligence

First, intelligence community surveillance assets—in space, in the air, on the ground, and underwater—could play a role in identifying and locating suspect vessels. These surveillance assets include systems that collect signals, imagery and communications intelligence, as well as other systems unique to the military services, particularly the Navy. There are also U.S. Navy assets, currently inactive, that could be activated to help cue other surveillance assets in tracking and locating maritime surface traffic. In addition, HUMINT capabilities are a valuable source of information about potential aggressors and their activities

Commercial

Second, data from a rich array of commercial sources, and collected through the regulatory and enforcement activities of the Department of Homeland Security, are a source of information on ships and containers that can help to improve container tracking and port security. By working with foreign governments and the shipping industry, the United States can obtain information on ships and containers before they leave foreign ports, with the effect of pushing border control away from the physical border of the United States. These data, combined with government filters provided by the Bureau of Customs and Border Protection's (BCBP's) Automated Targeted System, for example, could help to identify ships and containers that might deserve close attention.

Many programs for collecting commercial shipping data exist. Others, established in the Maritime Transportation Safety Act of 2002, are in the process of being implemented. Figure 9 shows key programs that influence maritime awareness in the littorals and U.S. ports, in transit, and in foreign ports. They include the following:

- The Customs-Trade Partnership Against Terrorism creates incentives for private companies to make their operations more transparent. With increased participation, BCBP can focus its resources on suspect transactions.

- Partnerships between the U.S. Coast Guard and the international shipping industry include an incentive-based program for foreign-flagged ships, known as Qualship 21, as well as cooperative arrangements with classification societies. Through these programs, the Coast Guard is able to collect a great deal of information about foreign-flagged ships.
- BCBP's container security initiative is expected to eventually cover 80 percent of containers coming to the United States; at present 15 nations have agreed to implement the initiative. This initiative, along with implementation of the International Ship and Port Security Code, will help to improve ship and port security.
- A 96-hour notice-of-arrival rule, implemented by the Coast Guard after September 11, 2001, provides earlier information about ships and crews.
- Implementation of the Automated Identification System (AIS) and the Global Maritime Distress and Safety System (GMDSS) tracking capability under the provisions of the Maritime Transportation Safety Act of 2002, will make it possible for the Coast Guard to track commercial shipping across the ocean in the not-too-distant future. Rules for implementation of GMDSS polling are expected by early summer 2004, with implementation to follow in 6 to 12 months.
- The AIS program will compel the owners of most commercial ships over 65 feet in length, foreign and domestic, to install an automatic identification system that will allow line-of-site identification when the vessel is within VHF-radio range (is less than roughly 30 miles away). The system's utility is limited to the immediate coastline, but can be an effective component of a broader system.

- Operation Safe Commerce, a Transportation Security Administration (TSA) program, represents initial efforts to track and monitor individual containers and encourages investigation of technologies to enable “in-transit transparency” in cargo container shipping.
- The Port and Maritime Security Act of 2001 requires the Coast Guard to conduct port vulnerability assessments, which have been ongoing since fiscal year 2002. The Maritime Transportation Security Act of 2002 mandates more explicit private sector contributions, including port and vessel security plans as well as designated security officers at facilities and aboard ships.

Defense Department and Coast Guard

The addition of DoD and Coast Guard intelligence, surveillance, and reconnaissance capabilities—including surface, space, air, and underwater assets—would be utilized by a maritime security system when a suspect ship or container on a ship closed in on U.S. shores. Assets from these organizations, joined as necessary by other interagency units and coordinated by means of a joint interagency task force, would be called upon to prosecute a potential target.

Joint Harbor Operations Center. The Joint Harbor Operations Centers (JHOCs) in Norfolk, Virginia and San Diego, California, represent positive advances in shared situational awareness for the immediate offshore and port regions. The San Diego JHOC has thus far used Coast Guard and Navy funding as well as support from Port of San Diego projects funded in part by port-security grants from TSA. The border patrol and San Diego harbor police also participate in this effort, which includes radar capability offshore and in port; video cameras placed throughout the harbor, some with thermal imaging capability; and some limited underwater detection capability. The San Diego project has developed a concept of operations that allows assets under different commands to participate

in a joint effort to monitor the immediate offshore and harbor and to coordinate the necessary response.

Maritime Intelligence Fusion Centers. The Coast Guard has established maritime intelligence fusion centers on each coast that bring together and analyze information from classified and unclassified sources. Their products feed the Office of Naval Intelligence/Coast Guard Intelligence Coordination Center effort that is known as the National Maritime Intelligence Center. This center provides intelligence to the U.S. Coast Guard, the U.S. Navy, and NORTHCOM's operations center, among others. Daily analyses of container shipping manifests, conducted by the DHS Bureau of Immigration and Customs Enforcement, are also used.

An Integrated Maritime Surveillance System

Figure 11 illustrates the combined, or federated maritime surveillance system envisioned. While new initiatives will enhance current capabilities, the challenge of developing an effective maritime surveillance capability is substantial. An integrated system will require seamless interfaces between DoD — particularly NORTHCOM and the U.S. Navy — and the Department of Homeland Security components involved in maritime security, principally the Coast Guard (the lead federal agent for maritime security), the Bureau of Customs and Border Protection (which provides for container security), and the Bureau of Immigrations and Customs Enforcement.

Such a capability need not involve the establishment of new operations centers, but it will require increasing integration of interagency operational forces. It will require a system-of-systems approach to ensure effective communication, data exchange, and operations between and among relevant nodes. The concept is to establish a system that can respond to a range of operational tempos — capable of sustained, normal operations and also able to surge to high intensity based on warning or for show of force.

To develop an integrated system, initial focus should be on existing and near-term capabilities. Collectively these initiatives will result in greater public and private awareness of maritime activity

and of more specific actions that need to be taken to maintain security and respond when breaches occur. The ultimate utility of these initiatives, as part of an integrated surveillance system, depends on sufficient resources and on cooperative arrangements to ensure that available data is effectively shared and used.

An Illustrative Scenario

The following scenario provides an example of how a federated system could skillfully manage a potential threat.

Daily analysis of manifest data from BCBP's Automated Targeting System reveals an anomaly about a particular container. The data is shared with the Coast Guard and the intelligence community via the National Maritime Intelligence Center. This cross-check reveals that the vessel carrying the container is of intelligence interest. Analysis of the integrated information leads to the conclusion that terrorists have a weapon in the container and are attempting to bring it into a U.S. port undetected. A search for the vessel is initiated, based on knowledge about container loading, vessel routing, and time of departure. The rapid escalation of interest in this vessel and timely sharing of information results in a seamless transfer to operational Coast Guard and Department of Defense assets to respond to the threat.

What this scenario illustrates is that analyses of commercial data, along with broader intelligence community analyses, could form the basis for judgments about ships and containers that might pose a threat to U.S. national security. When anomalies are detected that require a response, seamless processes must be in place and well-exercised in order to rapidly achieve the redirection of intelligence assets, DHS assets (such as the Coast Guard), and DoD maritime, air, surface, and sub-surface assets, in order to locate a vessel, board it, redirect it, or if necessary conduct military operations against it.

A Role for DoD

The DSB believes that the Department of Defense can make a significant contribution to developing a national capability that can

effectively respond to such a scenario. First, the Department needs to encourage and support interagency efforts via a maritime surveillance working group. DoD assets should be shared to support data-mining efforts of the BCBP and the Coast Guard. Both organizations are investing heavily in the tools required to conduct effective risk-management analyses of their data, and DoD should become involved in these efforts.

DARPA should work with DHS to ensure best practices on data mining from ship and container data. Where possible, the Department should support the Coast Guard's integrated deepwater acquisition program, particularly with respect to ensuring compatibility in sensor and communication gear between the Navy and Coast Guard. Finally, the Department should support the joint harbor operations center concept as developed in San Diego and Norfolk and explore its expansion to other strategic ports.

The maritime surveillance system described will not provide continuous tracking of all vessels. Such a goal is not practical. However, the system will significantly improve current capabilities and enhance homeland security.

RECOMMENDATIONS EXTEND MARITIME DEFENSE

The Secretary of Defense should task

NORTHCOM to take DoD lead in defining maritime surveillance requirements

NORTHCOM, in cooperation with other departments and Canada, to create a spiral development plan for an integrated maritime surveillance system

- Eventually include Mexico

Navy to examine use of low-frequency and broadband acoustics

NORTHCOM to review maritime surveillance requirements for the evolving Space Based Radar program

DEFEND AGAINST THE LOW-ALTITUDE AIR THREAT

Until recently, the threat to U.S. territory posed by cruise missiles and other low-altitude, air-breathing assets was treated as a sub-set of more troublesome long-range bomber and ballistic missile threats. However, since the end of the Cold War, the United States has enjoyed a commanding lead in all aspects of offensive and defensive air power. Moreover, effective, affordable U.S. ballistic missile defense capabilities are now being fielded and will deny most potential adversaries an important means with which to threaten the United States – intercontinental ballistic missiles.

In concert with other components of U.S. strategic military dominance, these changes have increased the attractiveness of cruise missiles and other low-altitude delivery systems as a low-cost, low-observable way for adversaries – especially non-state adversaries – to deliver biological and other mass-destruction weapons against U.S. targets.

Today, relatively sophisticated, short-range cruise missiles are increasingly available, as are the technologies needed to equip them with precision guidance and a range of weapon systems. For geographic reasons and to avoid detection and interception by the U.S. Coast Guard, sea-going vessels seem most likely to be the launch platforms for cruise missiles and other short-range delivery systems. If not countered, such delivery systems have the potential to penetrate existing U.S. defenses and attack targets without attribution. A national program for developing defenses against the low-altitude air threat is needed. DoD needs to develop an operationally feasible and cost-effective response to these sea-borne threats.

DoD is developing a number of high-quality missile defense technologies to defend against short and intermediate-range threats. The Patriot 3 (PAC-3) and Medium-Range Extended Air Defense System (MEADS) should, in the near future, provide DoD with the capability to destroy cruise missiles in flight. Just as important, various terrestrial, airborne and space-based radar technology improvement programs should, in the near future, provide DoD with

an ability to detect, track, and intercept individual cruise missiles and other low-altitude delivery vehicles. It is increasingly clear, however, that these technologies and systems must be integrated into a robust defensive architecture – one that is capable of operating in an area-wide as well as a point-defense mode. For this purpose, today's predominantly service-level programs need to be migrated into a national low-altitude air-defense program and architecture. The Joint Requirements Oversight Council has taken note of this requirement and is already exploring a number of policy and programmatic options.

Focus on Platforms

In the view of the DSB, because low-altitude air-defense systems cannot be everywhere, top priority needs to be given to defense against platforms – “killing the archer, not just the arrows.” This approach will require DoD to identify potential sources of cruise missiles and other low-altitude weapons platforms, launchers, warheads, and technologies. The necessary intelligence collection, processing, and analysis capabilities can be obtained by integrating DoD and non-DoD assets to support early identification and continuous monitoring and targeting of suspicious technology transfer, manufacturing, testing, purchasing, shipping, and other activities.

As discussed in the previous section, numerous maritime monitoring capabilities are fielded or being fielded in the relative near term, with the potential to support a layered, low-altitude air defensive system. To achieve a robust defense capability, U.S. Navy and other DoD intelligence, surveillance and reconnaissance assets and capabilities need to be integrated into this national maritime surveillance system. In this regard, DoD needs to resolve interagency issues such as who designs, builds, buys, and deploys which technologies, and who ensures they operate as components of a coherent system-of-systems.

Ensuring the U.S. Navy and Coast Guard are positioned and empowered to intercept suspicious bulk cargo and container ships is the next component of a platform-oriented maritime security

capability. For this purpose, DoD needs to commit the Navy to active participation in an extended maritime perimeter defensive architecture. The DSB recommends that DoD task NORTHCOM to serve as the combatant command responsible for command and control of any committed maritime forces.

Point-Defense Capabilities

Defending against the low-altitude air threat requires enhanced point-defense capabilities as well. However, a proliferation of point-defense systems is likely to be prohibitively expensive. Because these systems cannot be everywhere, all the time, robust indications and warning capabilities must exist for cueing and to enable the concentration of available low-altitude air-defense assets along high-threat corridors. GMDSS and other maritime indications and warning systems are already being pursued by DHS.

DoD's air- and missile-defense radar systems need to be fully integrated into the maritime surveillance architecture. As well, any future indications and warning architecture needs to include space-based radar systems, bistatic passive coherent location systems, and low-frequency, broadband underwater acoustic sensors. DoD will need to play a role in the acquisition and employment of these assets. The main point, however, is that the PAC-3 and MEADS systems—even in combination with a robust U.S. air-defense system—will only suffice if DoD assists other agencies in fielding a robust indications and warning system and in integrating this system into the broader national maritime surveillance system.

A near-term focus on platforms, combined with enhancement of point-defense systems, will establish a basis for rapidly deploying an effective defense capability against the low-altitude threat in the years ahead. Moreover, this two-track approach will enable DoD to assume a leadership role to field a fully integrated maritime security architecture as expeditiously as possible—and within that system, an affordable low-altitude air-defense capability.

RECOMMENDATIONS

DEFEND AGAINST THE LOW-ALTITUDE AIR THREAT

Accelerate development of a limited capability to permit periodic coverage based on indications and warning

Create a low-altitude air threat defense roadmap/master plan/concept of operations

- Assign lead to NORAD with JTAMDO and NORTHCOM support
- Require a supporting technology plan by USD (AT&L)

Task the Director, Central Intelligence, for a low-altitude air threat National Intelligence Estimate

- NORAD becomes a demanding customer

Do not create a major program office at this time

- Get the roadmap first
- But ensure maritime requirements are included in SBR development

Do not assign current service low-altitude air-threat defense programs to Missile Defense Agency at this time

NORTH AMERICAN DEFENSE COMMAND

In order to effectively operate the capabilities suggested above, and provide integration between air and maritime defense, the DSB recommends possible creation of an integrated North American Defense Command (NADC), which would evolve out of today's North American Aerospace Defense Command (NORAD). The rationale for creating an integrated (air and maritime), coalition between the United States, Canada and, at some point in the future, Mexico, can be best understood in terms of three operational requirements.

First, DoD's ability to successfully accomplish its homeland defense and homeland security missions will depend increasingly on its ability to coordinate its own air and maritime surveillance and intelligence gathering activities with comparable activities of the larger intelligence community; other federal departments including Commerce, Justice, and Homeland Security; as well as non-federal departments and agencies. Without sharing and collaborating on an interagency level, a robust maritime security and low-altitude air-defense capability may be neither feasible nor affordable.

Defense against these threats will almost certainly rely on cueing information provided by a variety of sources, which will need to be integrated to support an appropriate operational response. Collaboration will also enable more effective use of limited radar assets and interceptor missiles and aircraft—targeting their use to appropriate geographic areas and potential launch platforms.

The DSB believes that DoD is the appropriate lead for an interagency effort to create an integrated air and maritime surveillance capability. DoD leadership will help to ensure that the capability is fully integrated within a command that has the authority, responsibility and wherewithal to respond to the widest possible range of air and maritime threats to the continental United States.

Second, the participation of Canada, and eventually Mexico, in a new North American Defense Command would greatly enhance the effectiveness of U.S. air, land, and maritime defenses against low-altitude air threats, terrorists, drug trafficking and other security threats to all three countries. Mexico will probably eschew a U.S.-Canadian invitation to join such an integrated command at this time. But Canada and the United States have established a working group to study and develop and expanded functionality of NORAD, to include a maritime dimension.

DoD should do all that it can to encourage the active participation of both countries in a new coalition security-architecture. The creation of an integrated (coalition and interagency) defense command should become an easier task as low-altitude air threats

become better defined and as the threat posed by terrorism to all three countries is more appreciated.

The third reason for establishing the NADC is that anything less than an interagency-staffed, coalition, air- and maritime-defense command will require DoD to unilaterally address gaps and potential shortfalls in the existing U.S. defensive architecture. By placing the operational control of air and maritime defenses – with possible further expansion to land missions – under a single command, similar to NORAD, the United States will be able to

- Provide effective, affordable terrestrial and space-based radar surveillance of the extended sea, land, and air lanes from which future threats to the national security of all three states are most likely to emerge
- Coordinate secure, responsive command and control within the extended air, land, and maritime areas that are the responsibility of Canada and Mexico
- Extend the security perimeters of all three countries by expanding their abilities to monitor and, if needed, intercept threats to their territories
- Expand the focus of national homeland security enhancement efforts to include interagency responses to strategic, regional, and transnational threats

Even if the expansion of NORAD into a U.S.-Canadian-Mexican North American Defense Command proves impossible for political or other reasons at this time, the DSB recommends that, at a minimum, DoD seek to expand NORAD into a U.S.-Canadian air- and maritime-defense command. In the meantime, it is important for the United States to continue its current efforts with Canada in the Bi-National Planning Group and seek the participation of appropriate interagency components – such as the Coast Guard, Commerce, and Transportation – in this group.

The DSB further recommends that this new command include a capacity for direct interagency operational-level coordination. The command should support coordination of maritime security operations, for example, and facilitate coordination of DHS and DoD homeland security and homeland defense activities.

It is especially important that a North American Defense Command be manned and equipped to:

- Provide continuous global, data tracking on merchant and pleasure ships (over 65 feet in length) during their approaches to U.S., Canadian and Mexican waters
- Track and analyze the ports of call and declared cargo of merchant ships prior to their arrival in these waters
- Share appropriate intelligence on maritime operations between the United States, Canada, and Mexico
- Consolidate national response efforts when merchant vessels attempt to illegally transport people or equipment into U.S., Canadian, or Mexican waters
- Use real-time intelligence from the U.S. National Maritime Intelligence Center for correlation and fusion with Canadian and Mexican maritime information sources
- Provide direct connectivity into the evolving U.S. national maritime surveillance system and, when fielded, U.S. low-altitude air-defense systems

RECOMMENDATION
NORTH AMERICAN DEFENSE COMMAND

Consider creation of a North American Defense Command, which would evolve out of today's NORAD, to integrate air and maritime defense

CHAPTER 5. EMERGENCY PREPAREDNESS AND INCIDENT RESPONSE

DoD's role in homeland security extends beyond homeland defense to include, when directed, military support to civil authorities. Should the U.S. homeland be attacked, DoD could be called on to assist with incident response. Consequently there are many preparedness measures in which the Department should be proactively engaged. The DSB focused on four areas where enhancements in DoD need to be made. These areas, covered in turn in this chapter, are as follows:

- Defend against chemical, biological, radiological, nuclear, and high-explosive attack. The DSB focused in this study on biological weapons and nuclear dispersal devices.
- Create a medical surge capability. DoD's extensive network of medical facilities and personnel can contribute to a national surge capability.
- Improve communications operability between first responders and federal, state, and local agencies involved in emergency preparedness and incident response.
- Enhance Reserve Component capabilities to support the homeland security mission.

DEFEND AGAINST CBRNE ATTACKS

Terrorist activity and targeting trends suggest increasing support among terrorist organizations for incidents involving mass casualties. Attacks using conventional firearms and explosives, on civilian and military targets, by ideologically committed individuals, are evidence of this trend. However, there is also evidence that interest in unconventional or asymmetric weapons is on the rise. The sarin attacks in the Tokyo subway in 1995, the events of September 11,

2001, the anthrax mailings in October 2001, and the alleged efforts of al Qaeda to develop chemical, biological and radiological weapons are examples of a turn toward potentially more lethal and potent weapons which can also have the effect of creating widespread terror in civilian populations.

Detecting, identifying, and localizing devices or materials across the chemical, biological, radiological, and nuclear spectrum presents a significant challenge. Radically different technologies are required to respond to each type of threat. As a general rule, increased research is needed in phenomenology of detection, the inferential signatures of threat agents, and methods and techniques of active interrogation.

The Departments of Homeland Security, Health and Human Services (HHS), and Defense all have equities in these areas and important contributions to make in mounting an effective defense. It is therefore important that the three departments work closely together to address these issues in a coordinated fashion that serves the needs of the nation.

The DSB focused on two of the most dangerous threats: biological warfare and nuclear dispersal devices.

Biological Warfare

For some time, there has been only limited progress in dealing with CBRNE threats, at least in part because solutions have been viewed as being out of reach and "too hard." This is particularly true of the threat of biological warfare. In the past few years, however, several DSB and other studies have examined the issues in detail and have concluded that defense against biological attack is possible, though it will require a significant effort in research and development.⁷

⁷ DSB/TRAC Task Force on Biological Defense, June 2001; DSB 2001 Summer Study on Defense Science and Technology, May 2002; and DSB Task Force on Homeland Defense Against Bioterrorism, November 2002.

Within DoD, current biodefense technology development efforts are heavily weighted toward early detection, either with in situ detectors or with syndromic surveillance systems. Early detection of any attack is crucial to minimize fatalities and, within DoD, assure continuity of essential capabilities. For example, the mortality rate for anthrax exposure is substantially reduced if treatment can be administered prior to the onset of symptoms. Given the limitations and cost of current environmental sensors, detection of a biological attack is most likely to come from reports by primary care physicians observing symptoms, unless the attacker chooses to make the attack highly visible (for example by spreading the pathogen in very high densities or explosively).

At the same time that DoD has focused significant resources on developing sensor detection technology, work on other aspects of biological defense has proceeded and produced many promising developments. *However, the current focus on early detection needs to be balanced with efforts to prevent infection through vaccines and therapeutics.*

A number of vaccines and therapeutics under development could prove promising and support the concept of increasing investment in this area. For example, a new, safer, and more efficacious recombinant anthrax vaccine has already reached the late stages of development and should be ready for use in the next few years. A promising ebola vaccine has been tested successfully in primates. A second-generation, cell-culture-based smallpox vaccine is in development. These advances notwithstanding, it remains the case that safe, highly effective, and fast-acting vaccines are not currently available for any of the Centers for Disease Control and Prevention Category A biological threats.

Post-exposure prophylaxis and treatment depend on a few classes of drug, some of which (e.g., botulinus toxin antiserum) are in extremely short supply. In general, much more research and development work is needed on broad-spectrum vaccines, presymptomatic diagnosis, therapeutics, and remediation. While these needs apply nationally, and while the protections that would benefit civilian populations are in most ways similar to acknowledged requirements for DoD personnel, the unique

demographics of the military population may facilitate vaccine development and testing and could allow stockpiling of broad-spectrum antibiotics and antivirals that have not yet completed the rigors of testing by the Food and Drug Administration. There are a number of issues associated with development of vaccines and, to a lesser extent, therapeutics that also need to be addressed. High on this list are liability issues, which are of great concern to vaccine and pharmaceutical manufacturers.

The success of the latest smallpox immunization campaign implemented by DoD for its personnel, compared to the challenges faced in the civilian program to inoculate health workers in the United States, is a striking example of the special advantage that the DoD has in vaccine development and use. DoD vaccinated 400,000 personnel in a few months with only 18 complications and no deaths whereas the public plan to vaccinate 450,000 health care workers in 30 days has hit serious roadblocks. Approximately 35,000 health care workers have been inoculated since January 2003; a number of individuals in this group experienced serious complications or death.

Remediation is another aspect of defense against biological weapons. It is critical to all elements of the population and infrastructure, but addressing the remediation of DoD facilities is perhaps an area where the Defense problem is slightly simpler than the general case. Remediation is also essential to force projection, as DoD has a strong interest in preserving continuity of operations, dependent on ports, airfields, and critical infrastructure. It is also possible to conduct remediation exercises on Defense facilities with less disruption than in the civilian community.

RECOMMENDATIONS BIOLOGICAL WARFARE DEFENSE

Establish DoD/HHS partnership for improved medical surveillance and to accelerate pipeline for new diagnostics, therapeutics and vaccines

- Increase emphasis on integration of new medical surveillance technologies
 - Speed up the pipeline for making new fast-acting vaccines and therapeutics available
 - Involve DoD in BIOSHIELD program at HHS
-

Nuclear Dispersal Devices

Among the gravest threats to national security is the possibility of an adversary obtaining access to nuclear weapons or a sufficient quantity of highly enriched uranium or weapons-grade plutonium to construct them. The importation and successful detonation in an American city of even a low-yield nuclear weapon would result in tens of thousands of casualties, hundreds of billions of dollars in damage, tremendous loss of infrastructure, and irrevocable changes in the American way of life. The primary and only acceptable strategy for meeting this threat must be to prevent such attacks from occurring.

A lesser but probably more plausible threat is the detonation by terrorists of a radiological dispersal device (RDD, or "dirty bomb") that uses conventional explosives to disseminate radionuclides over a broad area. Dirty bombs could cause widespread contamination requiring temporary sheltering-in-place or evacuation of affected populations, cause mass disruption of services and commerce, and necessitate expensive long-term environmental mitigation and clean-up efforts.

The collapse of the Soviet Union raised concerns that Soviet nuclear weapons and stockpiles of fissile materials could move onto the international black market and become available to rogue nations and terrorist organizations. The alleged efforts of Iraq and al Qaeda

to develop RDDs raise special concerns about this class of device, especially given the fact that highly radioactive sources are present in large numbers in the United States and thus may be easier to access than obtaining highly enriched uranium and plutonium.

An End-to-End Response Strategy

Current technical capabilities for detecting nuclear dispersal devices are limited, and passive portal detection alone is insufficient to counter the threats of greatest concern. An end-to-end concept of operations that would produce a layered and integrated prevention and protection strategy needs to be developed. The goal is to prevent such weapons from reaching U.S. soil, because even with perfect detection capabilities within CONUS, a weapon in the United States would result in unacceptable risks to civilian populations and military personnel.

Currently, U.S. points of entry are treated by DHS as the first line of defense. Most of the nation's attention and resources are placed here. Traditional interdiction of contraband and collection of duties and tariffs consolidate the federal presence at the portals—a single point in the debarkation flow. At these points, agencies are subjected to intense pressures to move goods and materials to the market and their final destinations with minimal dwell time. As discussed earlier, any device landed on U.S. soil must be considered a terrorist victory as its detonation upon detection is deemed extremely likely.

Therefore, *the first line of defense must be beyond the territorial borders of the homeland*. While there are U.S. government extraterritorial efforts underway in key countries, more resources and attention must be placed here. It is beyond U.S. borders that the dwell time is the greatest: there are long slow lines to load vessels and aircraft for departure, enabling more careful inspection. This setting is in contrast to the point of debarkation, where the pace of unloading and entry to transportation and commerce systems is unrelenting.

Furthermore, DHS needs to put in place, wherever possible, additional first lines of defense at the outer edges of its jurisdiction. Here the dwell time is often greater, and the risks just identified in

interdiction processes are isolated off U.S. soil. As an example, used offshore platforms could be positioned beyond the openings to economically significant ports or areas important for force projection. Coast Guard crews could be sent by air to these platforms, where incoming vessels could be staged for inspection. Such an approach would push the zone of interdiction further offshore.

The U.S. border then becomes the second line of defense. At the border, processes need to be reconfigured to accommodate the possibility that an interdiction will trigger a detonation. Process-changes would involve amendments to local conduct of operations, changes in the location of inspections on site, modification to third-party observation of the portal processes, and potentially changes in personnel conducting all aspects of the facility's operations. Such process changes would offer higher immediate returns than additional effort spent on further improving the current detection regime.

The third line of defense, inside the homeland, receives the least amount of resources and attention at present. Yet there is much to be done. Most of the current portal surveillance data at the ports of entry are currently maintained in situ. A detonation of an improvised nuclear device (IND) on site could destroy all available surveillance and documentation necessary for a subsequent investigation. These resources must in every case be backed up off site to preserve them should an incident occur.

Local concepts of operations and exercises must include the possibility of missed detection at the first and second lines of defense of a device subsequently determined to be a threat. The procedures, responsibilities, and command-and-control issues for the non-federal players then involved need refinement before such an incident occurs. Analysis of takedown concepts-of-operation (intentional or otherwise) by non-federal personnel for RDDs and INDs, as well as a rapid investment in applicable technologies for use at the points of entry or en route to targets, are actions that need to be taken.

The combination of these steps will shift the focus from the search for terrorist materials to a search for weapons, from the U.S. points of

entry to those abroad, and from detection to consequence management. The result will be a lowered risk to the homeland and increased deterrence to terrorists for the use of these devices.

Current Capabilities of Note

The Armed Forces Radiobiology Research Institute. The Department of Defense possesses a unique national resource in the Armed Forces Radiobiology Research Institute (AFRRI), which is the only scientific institute in America that is dedicated to the development of radiation countermeasures and that has the capability to perform (and routinely does perform) research into uncontrolled radiation exposure. AFRRI has been undercapitalized for several years and prior budget cuts have significantly degraded its capability to perform needed research into new and promising countermeasures. DoD should increase funding to AFRRI and seek additional funding through cooperative arrangements with DHS and the Office of Biodefense Research Affairs at the National Institute of Health.

The Guardian Project. The Guardian project is a new, joint DoD force- and installation-security program to provide protection against chemical, biological, radiological, and nuclear threats. The project, which began on October 1, 2003, will assist commanders in providing CONUS and OCONUS force protection for U.S. military installations. Over the next five years, Guardian will address force protection of 185 facilities in the United States and 15 overseas. The project will define standards for protection, but tailor implementation according to installation needs. Design and installation of detection systems will be part of the program. The project extends to the surrounding civilian communities and first responders.

The Guardian Brigade. The Army is developing a new CBRNE response capability. The Soldier Biological Chemical Command is organizing a "Guardian Brigade," which will expand into the "Army CBRNE Command." The command will be prepared to provide full-spectrum homeland defense support to civil authorities. Army Forces Command will have administrative and operational control of the command. The command will be designed with capability for CONUS and OCONUS operations.

RECOMMENDATIONS NUCLEAR/RADIOLOGICAL PREPAREDNESS

Increase funding to the Armed Forces Radiobiology Research Institute (AFFRI) for development of radiological/nuclear medical countermeasures, radioprotectants, and improved bioassays

- Research should be coordinated with NIH, NCI and DHS

Acquire adequate stockpiles for military use of Prussian Blue, Ca-DTPA, Zn-DTPA, KI, and G-CSF⁸

A Coordinated Response to CBRNE

While many dispersed programs are addressing the CBRNE challenge, benefit would come from some centralization of responsibility. A central authority could serve as a focal point to draw in experts that can be brought to bear in the event of a major incident. It could ensure that the relevant programs underway are shared across the community. The DSB recommends that the following steps be taken.

RECOMMENDATIONS CBRNE

Assign responsibility for setting *requirements* for CBRNE defense of CONUS bases to NORTHCOM

Create a highly trained, multi-functional team at the federal level to broadly advise the executive branch in the event of a major CBRNE incident

- 50 to 100 people from within and outside government
- On call around-the-clock

⁸ Prussian Blue, Ca-DTPA (Trisodium calcium diethylenetriaminepentaacetate [DTPA]), and Zn-DTPA (Zinc-DTPA) are used to treat individuals who ingest or inhale certain radioactive materials. G-CSF (Granulocyte Colony Stimulating Factor) has been used to stimulate white blood cell production in patients receiving high doses of radiation. KI (potassium iodine) can help protect the thyroid gland from absorbing radioiodine in the case of a radiological emergency.

RECOMMENDATIONS CBRNE (CONT)

Establish a DoD/DHS/HHS partnership to incorporate the best technology and reduce time and cost for development/operation

- Integrate existing DoD and DHS capabilities for monitoring and response in selected locations
- Establish a distributed set of large-scale remediation assets that draw from DHS and DoD investments

Establish a shared technology base that connects advances in basic CBRNE technology development, prototyping and development

Increase effort to develop mobile, broad-spectrum neutralization and remediation technology—a suggested DARPA initiative

CREATE A MEDICAL SURGE CAPABILITY

Because of the current integration of military medical services with the civilian health care system, civilian hospitals, health care facilities and public-health agencies would inevitably be involved in responding to any mass casualty attack on a U.S. military base. (This is especially true where providing care for military dependents is concerned.) Consequently, the military's ability to limit casualties and maintain unit cohesion and operational flexibility following a widespread attack cannot be separated from the vulnerabilities of the civilian medical and public-health systems that serve base populations and neighboring communities.

Unfortunately, public health-care institutions and agencies are presently encumbered by downsizing pressures and priorities that limit their capacity to respond adequately in the aftermath of an attack of even modest proportions. *The implications of this vulnerability for maintaining Department of Defense operational capability have not been fully recognized.*

A robust capability for DoD to surge medical treatment is critical but lacking. The Department of Defense needs quantitative, end-to-

end plans for medical surge *for its own forces*. In addition, DoD has relevant medical and logistical expertise that, circumstances permitting, could be useful in support of civil missions.

National Disaster Medical System

The federal government's organized medical surge capability currently resides in the National Disaster Medical System—a cooperative arrangement between the Departments of Homeland Security, Health and Human Services, Veterans Affairs, and Defense. The system includes an essentially untested mechanism for the forward movement of patients as well as approximately 8,000 potentially deployable volunteer private-sector health care professionals and paramedics organized in Disaster Medical and Mortuary Assistance Teams (DMATs and DMORTs).

The capabilities of this system, while formidable, should not be overestimated: DMATs and DMORTs, of which there are about 60, are typically organized with 3:1 or greater redundancy to ensure that adequate volunteers are available for deployments. Deployed teams typically consist of about 30 individuals, including three or four physicians, and rotate every two weeks. Thus, federal resources to augment local authorities, while adequate for most naturally occurring or manmade disasters, would quickly be depleted by catastrophic or multi-focal events. Terrorist attacks with weapons of mass destruction would place immense strains on existing federal capabilities.

The speed and effectiveness of the medical and public-health response to an attack on U.S. forces will have significant operational and political consequences. The importance of limiting casualties and minimizing interference with military operations is obvious. In addition, effective medical and public-health measures will be critical to avoiding widespread fear and minimizing social and economic disruption. Failure to deliver adequate medical care or to execute appropriate public-health measures could lead to loss of public confidence in the government's ability to protect civilian populations, raise the possibility of profound, even violent, civil disorder, and possibly erode U.S. strategic flexibility.

Implementing Medical Surge for DoD Force Protection

To protect its own assets and ability to project force, the DoD needs to develop a robust capability to surge medical treatment both to bases and to critical ports of departure. Dependence on civilian institutions cannot be allowed to jeopardize operational capabilities. Moreover, an effective medical surge capability could limit the catastrophic consequences of an attack. DoD possesses the medical and logistical expertise to assume this urgent responsibility, including mechanisms for transporting medical materials, training medics and delivering care under difficult conditions and in austere environments.

A critical first step in acquiring appropriate surge capacity will be delineation by DoD of reference scenarios – representative, hypothetical emergencies – that will facilitate the development of a quantitative end-to-end solution to this problem. Reference scenarios should focus on response to major biological and radiological attacks on DoD CONUS and OCONUS facilities.

Figure 12 offers an example of a reference scenario, with an illustrative military pre-event checklist. This particular scenario involves the point release of one gram of anthrax against the Army base at Ft. Riley, Kansas. The shaded areas show the region that would be affected by the attack, based on weather data from August 8, 2003. The various shades on the map, from light to dark, indicate increasing concentrations of spores, which define the population that would be affected and the percentage of that population who would receive a lethal dose.

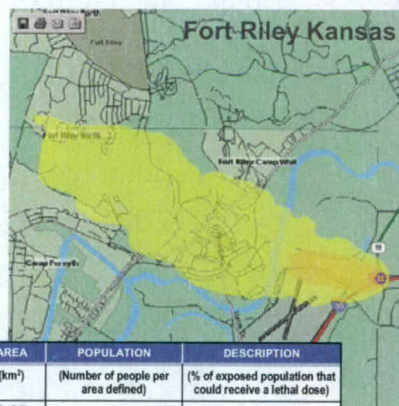
While the casualties in this scenario are relatively low, the effect on a more densely populated area would be much more significant. In addition, a more carefully coordinated attack might have more devastating effect if it utilized a line-release or if it were conducted during meteorological conditions more conducive to the spread of the agent. DoD must also carefully consider scenarios involving attacks that would have implications on U.S. force projection from places like Ft. Riley. Planning should also take into account the possibility of a concerted campaign of attacks – such as the use of

biological, radiological, chemical, and/or high-explosive weapons in conjunction with or complemented by cyber attacks and information operations. The *DSB Task Force on Homeland Defense Against Bioterrorism* proposed four practical scenarios that could form the starting point for such planning⁹.

Figure 12: Example Reference Scenario

Military Pre-Event Checklist

- Pre-event readiness
 - Detection assets and procedures
 - Planning, training and exercising
 - Inoculation and stockpiling
- Incident response
 - Detection
 - Characterization
 - CONOPS
- Surge requirements
 - Containment (ring, relocation, quarantine)
 - Medical treatment
 - Sustainment
 - Psychological
- Recovery requirements
 - Decontamination
 - Safety re-certification
 - Re-cock (and lessons learned)



LEVEL (Colony Forming Units per m ³)	AREA (km ²)	POPULATION (Number of people per area defined)	DESCRIPTION (% of exposed population that could receive a lethal dose)
>530,000	0.05	2	50
>17,000	1.2	49	15
>630	13.5	1,448	2

Taking an end-to-end approach to developing a medical surge capability will allow DoD to develop a detailed concept of operations, a description of the equipment and personnel needs, and an R&D plan to close identified gaps in capabilities and identify new medical needs and incident management tools. The results of these analyses should be shared with DHS, HHS, and Veterans Affairs (DoD's partners in the National Disaster Medical System), to seek their involvement and advice.

Despite its essential focus on the protection of military assets, the DoD plan for base installation protection and incident management must recognize that its activities will, in all likelihood, extend "beyond the fence." Therefore the plan must involve coordination with local and state civilian authorities. Together with these authorities, the plan must be validated by gaming, red teaming, and

⁹ November 2002.

realistic exercises. Because of DoD's current vulnerability and the urgency of the situation, *the first draft of the DoD medical surge plan should be completed by the Assistant Secretary of Defense for Health Affairs (ASD[HA]) for OSD review by June 2004.*

In drawing up its medical surge plan, the ASD(HA) should also consider current national initiatives and reports that may be relevant to this plan. Such initiatives include

- BIOSHIELD
- National Disaster Medical System
- Federal medical stockpiles
- The Bioterrorism Hospital Preparedness Program

RECOMMENDATIONS MEDICAL SURGE

A joint, interagency stockpile management is needed that includes DoD, HHS, DHS, and the VA

ASD(HA) and ASD(HD) should support development of an operations plan for a DoD medical surge capability, responsive to CBRNE attacks on DoD facilities

- Policy development
 - Resources to develop the plan
 - Review plan and identify resources in the 2005 POM to execute
-

RECOMMENDATIONS MEDICAL SURGE (CONT)

Secretary of Defense should task the ASD(HA) to designate the lead systems engineer and manager of the medical surge plan development. Requires detailed coordination and integration with

- Service surgeon generals and other service entities
 - HHS, DHS, Veterans Affairs, state and local governments
 - U.S. Northern Command, U.S. Joint Forces Command, and U.S. Transportation Command
 - Army Corps of Engineers and others
-

IMPROVE COMMUNICATIONS OPERABILITY

Communications for military assistance to civilian authorities (MACA) presents a unique challenge and opportunity for DoD. Civilian authorities include the civilian parts of the federal, state, and local governments; tribal authorities; and a diversity of private-sector organizations including both agencies and individuals. Communications between DoD and these various entities could be crucial in the case of a shared emergency.

A pervasive communications infrastructure exists in the United States, permitting communications via radio and television broadcast, cellular telephones, wired telephones, a wide range of two-way radios that are both analog and digital, and the Internet. The Internet is becoming increasingly connected with other communications systems and in some cases replacing them. The Internet includes both wired and wireless access to an increasing range of end user devices and advanced services. While these diverse communications systems are increasingly pervasive, they are generally not interoperable or suitable for use in critical situations to protect life and property.

The near-term challenge is to achieve effective communications for critical applications in case of emergency, to enable interoperable

command and control within the civilian sector and between the civilian sector and the Department of Defense, when its assistance is needed. Effective communication tools are needed throughout the entire life cycle of an emergency – from pre-event indications and warning, throughout the event itself, and in the aftermath during recovery efforts.

NORTHCOM and the National Guard, in cooperation with the Department of Homeland Security, have a leadership role to play in establishing effective operability standards and in deploying critical assets. In addition, there is an opportunity for the private sector to provide enhancements to end user devices and other commercial products in the information infrastructure – to include the Internet and systems deployed using the Internet technology base. Early involvement of the commercial sector will enable accelerated development of cost-effective and highly functional products that can gracefully transition from day-to-day applications to critical applications when needed.

Project SAFECOM

SAFECOM – an interagency initiative led by DHS – provides a near-term capability for enabling effective interoperation of existing wireless communications devices and systems, including their interface to the wired command-and-control system. Such a system has the potential to improve overall situation awareness among first responders and to provide decisive information in a timely way, essential for saving life and property in a crisis. However, SAFECOM has limitations because it does not address critical communications security issues and could become a natural target for an adversary who recognizes the role of communications in critical situations.

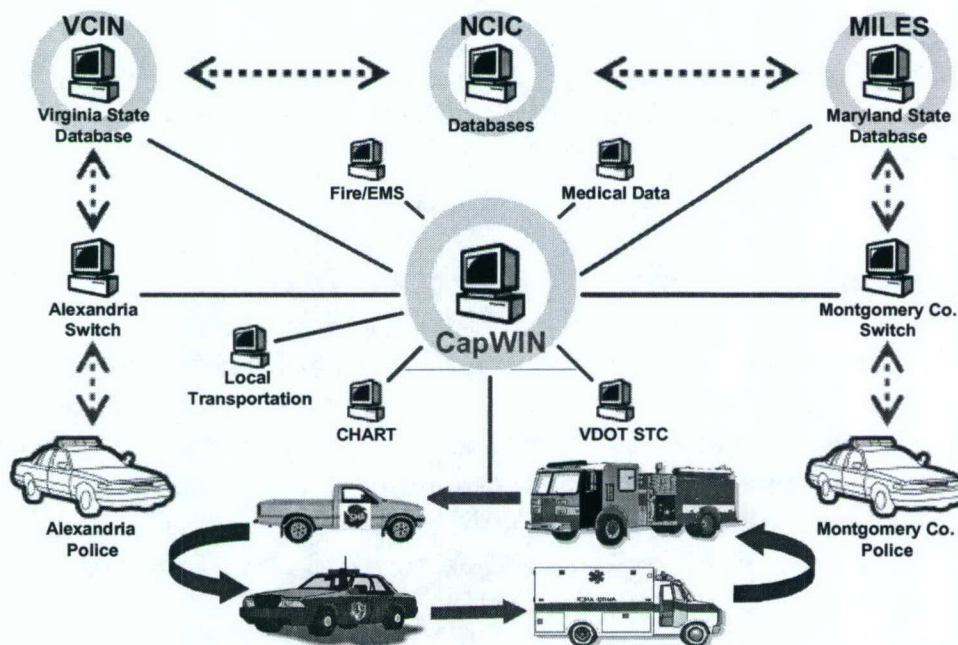
An open standards process, combined with experimental pilot projects in realistic settings, is essential for accelerating the development of SAFECOM in the near term. For the longer term, the SAFECOM capability should be extended to interoperate with public communications systems in order to provide designated first responders with the critical capabilities they need. The future

systems will provide significantly enhanced performance while also saving time. Rapid deployment of emergency wireless capability will enable increased readiness in preparation for an expected event, in response to an actual event, and in the recovery process.

CapWIN

SAFECOM provides oversight of local initiatives such as the Capital Wireless Integrated Network (CapWIN) Initiative, depicted in figure 13. The goal of this initiative is to develop an integrated mobile wireless network infrastructure, using a partnership among transportation and public-safety agencies in the Washington, D. C. metropolitan region.

Figure 13. CapWIN Provides Enhanced Mobile Communications and Information Access



The system will facilitate mobile communications and enable a properly authorized user to readily access and use information regardless of its location in national, state, or local databases. If successful, the program should enhance response capabilities of

transportation, law enforcement, fire, and medical first responders involved in critical incident responses. The network will also provide critical information to public-safety and transportation officials dealing with life-threatening situations.

This system, which is expected to be operational within a year, could be a model for other regions in the United States, and is being developed and documented with this potential in mind. Already, several cities and regions have expressed interest in a CapWIN-like capability.

RECOMMENDATIONS

IMPROVE COMMUNICATIONS OPERABILITY

NORTHCOM and the National Guard should proactively support DHS in establishing effective operability standards and in deploying critical communications assets

DHS and civil agencies should adopt SAFECOM and CapWIN approaches as a near-term capability for enabling effective interoperation of existing wireless communications devices and systems

ENHANCE NATIONAL GUARD CAPABILITIES

By nature, emergency response is local. Therefore, the national strategy for homeland security requires robust local, state, and regional preparedness. DoD has a forward-deployed, community-based military force with long-standing, mature relationships with principal players in the domestic emergency response community that can be used for homeland defense and MACA missions. This resource is the National Guard.¹⁰

National Guard units, bases, and supporting infrastructure are embedded in nearly 3,300 locations and 2,700 communities nationwide. This distributed, integrated defense force can provide a

¹⁰ Volume II contains more detail on the homeland security activities of the individual Reserve Components and the individual initiatives summarized in this chapter.

fiscally and operationally efficient means to contribute to national preparedness. With adequate resources, the Guard is optimally suited to contribute to DoD's homeland security missions. In fact, a number of ongoing National Guard initiatives will support homeland security operations.

Joint Standing Headquarters

In an effort to improve command and control, the National Guard was transformed, in July 2003, into a joint bureau with a joint staff. The separate Army and Air National Guard headquarters in each state are being replaced by a single, streamlined Standing Joint Force Headquarters. The joint staff of the headquarters will include title 10 personnel, including Army, Navy, Air Force and Marine Corps personnel – and title 14 Coast Guard personnel. The DSB recommends that Emergency Preparedness Liaison Officers, Defense Coordination Officers and Joint Reserve Augmentation Detachments be assigned to the Joint Forces Headquarters in each state and report to NORTHCOM.

Civil Support Teams

The joint Air-Army Guard Weapons of Mass Destruction Civil Support Teams (WMD-CSTs) are a critical, special-purpose resource that could be used for homeland security missions. The 22-member teams are capable of conducting on-site sampling and evaluation of hundreds of potentially lethal CBRNE threat agents and providing technical information and advice to incident commanders and other emergency responders. These teams can be deployed on a 24-hour-a-day basis and have advanced mobile communications suites, capable of interacting with other emergency responders and of reaching back to CONUS to subject-matter experts.

There are currently 33 certified teams in 32 states. The 107th Congress authorized, but did not fund, a total of 55 teams, which includes teams for each of the 23 states that currently do not have teams. The DSB recommends that the remaining 23 teams be funded and activated as quickly as possible. In addition, the laws restricting use of the civil support teams in CONUS only should be amended to

allow limited overseas deployment in support of combatant commanders in an emergency.

The DSB also encourages the Secretary of Defense to task the Chief, National Guard Bureau, to report to him on the feasibility of expanding ten of the CSTs so that each of the ten has a full, single-unit capability roughly equivalent to that of the Marine Corps' Chemical, Biological Incident Response Force (CBIRF). This augmentation would permit strategic positioning of ten additional CBIRF-equivalents throughout the United States, while leveraging the Guard's command-and-control and operational integration with the civilian emergency response community.

Joint CONUS Communications Support Element

The National Guard, with support of the 54 adjutants general, has been working with NORTHCOM on the Joint CONUS Communications Support Element (JCCSE) to enable shared situational awareness in support of homeland defense and MACA missions. NORTHCOM has been a principal player in the development of the requirements for a robust, flexible, reliable communications architecture able to reach any incident site.

The National Guard will be both a contributor to and user of the JCCSE. The Army and Air National Guard have information technology capabilities that can be leveraged to extend this trusted information environment from the DoD enterprise level to the state level and to that of the incident site. Because of its community-based presence, the Guard will also have a need for timely access to information and collaboration tools in order to effectively carry out its mission. Responding to both National Guard and NORTHCOM requirements, the JCCSE architecture should include a long-haul network (GIG-BE), as well as a wireless local area network, such as SAFECOM, which was described in the previous section.

The Secretary of Defense, through the Chairman, Joint Chiefs of Staff, should direct the Commander, NORTHCOM to create the JCCSE. Further, the National Guard Bureau should be tasked to develop and operate the JCCSE as a national mission in support of

OSD and NORTHCOM. The capabilities managed by the JCCSE will support DoD's homeland defense and homeland security requirements, but they can also be leveraged to provide information-sharing capabilities to other federal agencies in support of the National Response Plan and the National Incident Management System.

Employing Guard and Reserve Forces

To effectively make use of the Reserve Components in support of homeland security missions, NORTHCOM planners should have a complete database of Reserve Component units and facilities. This database – which should include unit and facility capability and availability – should be compiled and updated by the individual Reserve Components. The data, once compiled, should be shared with adjutants general and Standing Joint Task Headquarters in each state.

The DSB believes that the best course of action is to use the Guard to the maximum extent possible in title 32 status for all federal-purpose domestic operations. This approach was used in executing the airport security mission in the immediate aftermath of the September 11, 2001, terrorist attacks. There are numerous fiscal and operational advantages to using the Guard in title 32 status – principal among them are the time savings involved in employing Guard forces under the existing state command structure and the ability to use volunteers without having to involuntarily mobilize units.

**RECOMMENDATIONS
NATIONAL GUARD AND RESERVE**

Secretary of Defense should support the following National Guard initiatives

- Expand the Civil Support Teams to all 54 states and regions
- Expand the role of ten (10) CSTs, each with a full single unit CBIRF capability
- Stand up of the Standing Joint Headquarters in each state and territory

Secretary of Defense should, through the Chairman, Joint Chiefs of Staff, task the Commander, NORTHCOM to

- Create a JCCSE
- Involve the National Guard in developing and operating the JCCSE to fulfill the mission

NORTHCOM planners should have a complete database of Reserve Component units and facilities

- Compiled and updated by the individual Reserve Components
- Data should include unit and facility capability and availability
- The databases should be shared with Adjutants General and Standing Joint Headquarters in each state

Emergency Preparedness Liaison Officers, Defense Coordinating Officers and Joint Reserve Augmentation Detachments should be assigned to the Standing Joint Headquarters in each state and report to NORTHCOM

The National Guard should be used in title 32 status to the maximum extent possible for all domestic operations

CHAPTER 6. EXPORTING DoD CORE COMPETENCIES

Earlier chapters in this report have emphasized what DoD needs to do to fulfill its own homeland defense and security responsibilities and what help it needs from others. This chapter turns to how the DoD can enhance homeland security by “exporting” relevant core competencies that match the needs of other organizations (federal, state, and local) with homeland security responsibilities. The DSB identifies three of these core competencies: training and exercises, experimentation, and operational-level planning and execution.

TRAINING

A persuasive case can be made that training (and its complementary exercises) is the most important factor distinguishing the capabilities of the U.S. military from those of other nations. Facilities and simulations are essential, but more significant is the training culture (and supporting standards) that has evolved over the years. The training that occurs at the National Training Center, at Nellis Air Force Base, at Fallon Naval Air Station, at 29 Palms and in the combatant commands’ exercises is evidence of this culture.

These training exercises are not “feel-good” or “show-off” activities, but learning experiences for all involved. Exercises provide real-time feedback and hardheaded assessment—fostering adaptability rather than rote learning. Formidable red teams (surrogate opposing forces) play vital roles in the training process. While effective training is not unique to DoD, few, if any, organizations have been as successful at leveraging its power and embedding it within the culture of the enterprise.

EXPERIMENTATION

Experimentation is still a maturing competency at DoD, but the Department’s experiences would be valuable to other organizations. Experiments are needed to explore new operational concepts, identify

risks and help guide investment decisions. Experiments can also identify flaws before they are exposed in real-world operations. Concepts can fail, but experiments fail only if nothing is learned. Sustaining such an ideal is difficult in large organizations, and DoD is no exception in this regard. Yet its experiences in conducting experiments and making use of what is learned from them would be of value to other organizations that need to embark on experimentation.

The notion of coevolving (“spiral developing”) concepts, tactics, organization, training, and leader development along with materiel and technology is as relevant to achieving enhanced homeland security capabilities as it is to more traditional military missions. This is an area where the DoD should work very closely with other agencies as it goes about designing its own homeland-defense and security-related experimentation.

OPERATIONAL-LEVEL PLANNING AND EXECUTION

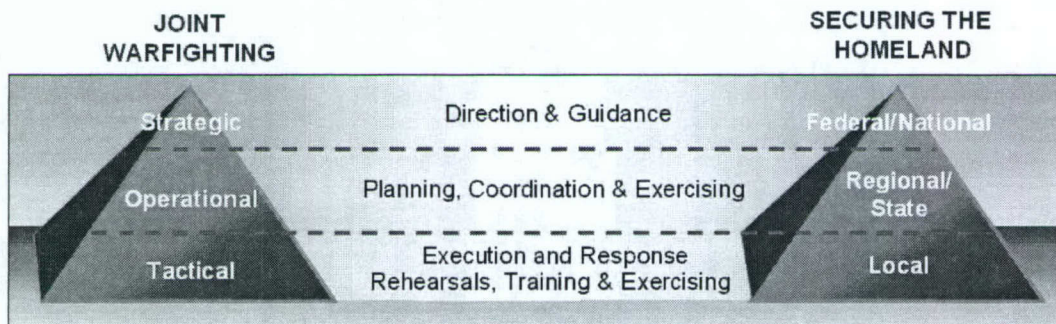
Operational-level commanders and their staffs compose and orchestrate tactical actions to meet national objectives and strategies and deal with uncertainty and adaptive adversaries. Composing and orchestrating tactical actions is inherently a joint activity for warfighting.

The major combat phase of Operation Iraqi Freedom showed the extent to which DoD’s capabilities for operational-level planning and execution have evolved. The aforementioned training and exercising play vital roles, as do professional military education and organizational constructs. One of these constructs is the joint task force approach that the DoD has refined over the years to prepare for and conduct complex operations. In a few cases, perhaps most notably the joint interagency task forces for counter-drug operations, the approach has been successfully applied to a multi-agency activity.

The Department of Homeland Security may find that standard interagency, Washington D.C.-based processes are inadequate for many of its responsibilities. Instead a more operationally oriented,

joint-task-force-like approach could be employed to address many areas discussed in this study. As shown in figure 14, the homeland security equivalent of the joint operational level for joint warfighting lies at the regional and state levels.

Figure 14. Opportunities for Exporting DoD Core Competencies Lie at the Tactical and Operational Levels



MAKING IT HAPPEN

How can DoD export these core competencies to other organizations?

First, the goal of exporting core competencies should be assigned as a high-priority responsibility to U.S. Northern Command and U.S. Joint Forces Command, with appropriate authorities. The DSB recognizes that this responsibility is not currently assigned to DoD and could result in opportunity costs for DoD missions. Nevertheless, the potential payoffs for protecting the nation are sufficiently great for the DoD to exert leadership in these areas.

Second, DoD will need a close partnership with DHS, not only to directly affect organizations within DHS, but also so that DHS may serve as the conduit to reach the regional, state, and first-responder communities. The National Guard—given its title 10 and title 32 responsibilities—can also play a key role.

RECOMMENDATIONS
EXPORTING DoD CORE COMPETENCIES

Assign overall responsibility for exporting core competencies to U.S. Northern Command and U.S. Joint Forces Command

The Secretary of Defense and Chairman, Joint Chiefs of Staff should assign the following areas of responsibility to the indicated organizations:

- Operational planning and red teaming
(NORTHCOM lead)
 - Joint Forces Staff College educational track for homeland security
(JFCOM lead)
 - Requirements for homeland defense experimentation
(NORTHCOM lead, with JFCOM assist)
 - Development of homeland security experimentation plan and initial execution (DHS lead, with JFCOM assist)
 - Interagency exercises for homeland defense
(NORTHCOM lead)
 - Training and inspection standards for homeland defense tasks
(NORTHCOM lead, with JFCOM assist)
-

CHAPTER 7. AN EVOLVING ROLE FOR NORTHCOM

In the past, the Defense Science Board has been accused of recommending the assignment of all unmet challenges to U.S. Joint Forces Command. Various DSB task forces may not have been right in all of the details or their recommendations, but their major message was correct: JFCOM needed to be empowered to serve as an agent for transformation. A similar circumstance exists now regarding homeland defense and security and the role of the U.S. Northern Command.

In this study, the DSB has recommended fifteen new tasks for NORTHCOM. Directing NORTHCOM to embark on all of these new tasks now is not feasible. Priorities are needed and are addressed below. *The main message is that NORTHCOM must be empowered for the nation to achieve its homeland security and homeland defense goals.*

The DSB recommends that the following four tasks be assigned to NORTHCOM now, with appropriate authorities and resources:

- Develop an integrated plan for maritime surveillance
- Develop a low-altitude air threat defense roadmap
- Take the operational lead for DoD mission-critical infrastructure protection in CONUS
- Take the lead for homeland-defense and MACA-related exercises, training, experiments and standards

Dealing with these four tasks (including the low-altitude air threat, which has civil aviation implications) will require extensive DoD-DHS interaction. NORTHCOM must be a major participant in these dialogues. The interactions should include unfettered dialogue about new ideas and concepts between NORTHCOM and DHS staff at all levels. (Any concerns about commitment of DoD resources can be handled by guidelines from OSD). The intent should be to foster the free flow of ideas and discussion between these two departments

of the U.S. government that share responsibilities for protecting the homeland.

The other recommendations for new NORTHCOM activities made by the DSB in this study are listed below:

- Sponsor information-sharing ACTD
- Review maritime surveillance requirements for Space Based Radar
- Support expansion of NORAD to North American Defense Command
- Adopt Joint Tactical Radio System as the standard tactical communications systems for MACA
- Assume responsibility for unique CBRNE requirements in CONUS
- Create a Joint CONUS Communications Support Element
- Develop a comprehensive database of Reserve Component capabilities and availability
- Develop training standards for DoD units designated for emergency response
- Develop interoperability standards for MACA for civilian responders
- Develop a guide for communication interfaces with each state and territory
- Assume duties as rear area coordinator for forward regional combatant commanders

CHAPTER 8. IN CONCLUSION

The preceding chapters of this report discussed ten areas, summarized in table 1, where initiatives need to be established by DoD to develop effective homeland security capabilities. The report has detailed specific recommendations and tasks in each area and has identified those tasks where partnership between the Department of Defense, Department of Homeland Security, and other federal and non-federal agencies is needed.

Table 1. Priority Areas for Homeland Security/Homeland Defense Initiatives

Global Situation Understanding	Share and assure information Create a potent HUMINT capability
Protect Critical Infrastructure	Protect DoD mission-critical infrastructure
Deter and Prevent Attack	Extend maritime defense Defend against the low-altitude air threat The North American Defense Command
Emergency Preparedness and Incident Response	Defend against CBRNE attack Create a medical surge capability Improve communications operability Enhance National Guard capabilities
Cross-Cutting	Export DoD core competencies Empower NORTHCOM

The DSB envisions a holistic, institutionalized approach to homeland security and homeland defense for the Department of Defense in the future. Elements of that vision, with four key areas highlighted, include the following outcomes:

- *DoD is able to focus on making every contingency an away game*
- NORTHCOM becomes a fully developed combatant command
- Greatly increased anti-terrorism capability and effectiveness for the Department of Homeland Security

- Matured supporting and supported relationships and interagency mechanisms
- Private sector actively engaged in security
- *Robust critical infrastructure program*
- *Redefined role of the National Guard and Reserves*
- *Integrated information sharing and command and control with state and local authorities*

By reaching this vision, the nation can turn a “yellow-orange” homeland security condition into one that is “blue-green.”

APPENDIX I. TERMS OF REFERENCE



ACQUISITION,
TECHNOLOGY
AND LOGISTICS

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

06 JAN 2003

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference - Defense Science Board 2003 Summer Study on the DoD Roles and Missions in Homeland Security

You are requested to form a Defense Science Board (DSB) Task Force addressing the Department of Defense (DoD) roles and missions in homeland security.

DoD's historic missions of homeland defense and civil support are under review in light of grave terrorist and other threats to US territory and citizenry. The DoD has access to many of the systems engineering, technical capabilities, relevant technologies, logistics expertise, and modeling and simulation capabilities needed for effective homeland security. Defense forces are also critically dependent upon various infrastructures operated by DoD or provided by commercial sources and civil utilities to support its force projection war-fighting mission and also provide force protection to forces stationed within the homeland.

The development of an effective homeland security capability will involve not only the Department of Defense but the direct participation of many other existing federal, state and local agencies as described in the "National Strategy for Homeland Security," Office of Homeland Security, July 2002.

Some of the key questions related to homeland security, which will be addressed by this DSB 2003 Summer Study, are:

- a. What is "homeland defense" and what specific roles and missions will the Department of Defense (DoD) be responsible to accomplish? What are the derivative unique operational responsibilities of US Northern Command?
- b. What are the prioritized goals for DoD support to civil authorities in a national security emergency? What are the derivative unique operational responsibilities of US Northern Command?
- c. What is the role of the National Guard and Reserve in homeland security? What are the implications for their warfighting mission?



d. What are the inter-agency processes that need to be put in place to support an integrated security strategy, planning function and operational capabilities? What are the processes for interacting with State and local governments?

e. What are the specific information sharing/fusion requirements with DoD and other governmental and non-governmental agencies? Define the processes and evaluate potential technologies to accomplish this requirement. Determine the optimal communications/hardware architectures.

f. What refinement is needed of theater security cooperation methods with Canada and Mexico? What are the short term and long term optimal goals with respect to homeland defense and military assistance to civil authorities for U.S. cooperation with these countries? Suggest a strategy to achieve these goals that addresses treaties, trade, relations, and impacts.

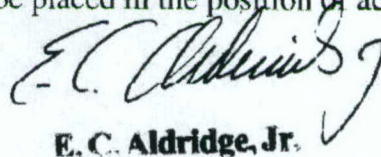
g. There are known and many unknown vulnerabilities regarding DoD force projection. How will projection issues and responsibilities be addressed in the larger context of homeland security?

h. What are the classes of technologies and systems that DoD should have the lead in developing and fielding which have applications for homeland security as well?

Other areas to be addressed by the 2003 Summer Study include: emergency preparedness and response, defending against catastrophic threats, and consequence management in dealing with weapons of mass destruction (chemical, biological and nuclear).

This study will be co-sponsored by me as the Under Secretary of Defense (AT&L), Assistant to the Secretary of Defense (Nuclear, Chemical, and Biological Defense Programs), Under Secretary of Defense (Policy), and Northern Command (NORTHCOM). The study will be co-chaired by Mr. Donald Latham and Admiral Donald Pilling, USN (Ret). Mr. Paul Bergeron, DATSD Chemical/Biological/Defense, Colonel Neal Anderson, NORTHCOM, and Lieutenant Colonel Craig Costello, Homeland Security Task Force, will serve as Executive Secretaries. Lieutenant Colonel Scott Dolgoff, USA, will serve as the Defense Science Board Secretariat Representative.

The Task Force will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, the "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of section 208 of Title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as procurement official.



E. C. Aldridge, Jr.

APPENDIX II. MEMBERSHIP

CO-CHAIRMEN

Mr. Don Latham	General Dynamics
ADM Don Pilling, USN (Ret.)	Logistics Management Institute

EMERGENCY PREPAREDNESS AND RESPONSE PANEL

Panel Co-Chairs

Dr. Richard Hatchett	Department of Health and Human Services
----------------------	---

Gen Michael Williams, USMC (Ret.)	Logistics Management Institute
-----------------------------------	--------------------------------

Members

Dr. Stan Alterman	Alterman Associates, Inc.
MG John Fenimore, USAF (Ret.)	The Fenimore Group LLC
Dr. Joshua Lederberg	The Rockefeller University
Mr. Larry Lynn	Private Consultant
Dr. Thom Mayer	INOVA Fairfax Hospital
Det. Todd Metro	New York City Police Department
Chief Edward Plaughner	Arlington County Fire Department
Dr. Anna Marie Skalka	Fox Chase Cancer Center

Government Advisors

COL Richard Marchant, USA	Force Transformation Office
---------------------------	-----------------------------

INFORMATION SHARING PANEL

Panel Co-Chairs

Dr. Joe Markowitz	Private Consultant
Mr. Larry Wright	Booz Allen & Hamilton

Members

Mr. Jim Gosler	Sandia National Laboratory
Mr. John Grimes	Raytheon Company
LTG Pat Hughes, USA (Ret.)	PMH Enterprises LLC
MajGen Ken Israel, USAF (Ret.)	Lockheed Martin

LTG Jim King, USA (Ret.)	MZM, Inc.
Mr. John MacGaffin	Private Consultant
Dr. Roy Maxion	Carnegie Mellon University
VADM Mike McConnell, USN (Ret.)	Booz Allen & Hamilton
Ms. Judy Miller	Williams & Connolly LLP
Mr. Bob Nesbit	MITRE
Dr. Pauletta Otis	Colorado State University
Dr. Terry Thompson	Private Consultant

Government Advisors

Dr. Alenka Brown-Van Hoozer	Oak Ridge National Laboratory
Dr. Richard Gault	DIA
Ms. Rosanne Hynes	OASD(HD)
Mr. Paul Ryan	DTIC
Ms. Carlynn Thompson	DTIC
Ms. Michelle Van Cleave	OUSD(Policy)

INTERAGENCY PANEL**Panel Co-Chairs**

VADM David Frost, USN (Ret.)	Frost & Associates Inc.
RDML Jim Van Sice, USCG	HQ NORTHCOM/J3V

Members

Mr. Dan Gallington	Potomac Institute for Policy Studies
Dr. Ralph Hallenbeck	Science Applications International Corp.
MG Ron Harrison, USA (Ret.)	Harrison and Associates LLC
Col Randall Larsen, USAF (Ret.)	ANSER Institute for Homeland Security
ADM William Studeman, USN (Ret.)	Northrop Grumman Systems and Information Technology Group
Mr. Chris Williams	Johnston & Associates

Government Advisors

Mr. Robert Earl	Department of Homeland Security
-----------------	---------------------------------

ROLES AND MISSIONS PANEL**Panel Co-Chairs**

Dr. Ted Gold	Institute for Defense Analyses
GEN William Hartzog, USA (Ret.)	Burdeshaw Associates, Inc.

Members

Mr. Samuel Adcock	EADS, Inc.
Mr. Michael Bayer	Private Consultant
Mr. Denis Bovin	Bear, Stearns & Co. Inc. Investment Banking
Dr. Craig Fields	Private Consultant
Mr. Robert Fitton	Resource Consultants, Inc.
LTG William Hilsman, USA (Ret.)	Private Consultant
Dr. David McIntyre	ANSER Institute for Homeland Security
Dr. Bert Tussing	U.S. Army War College
Ms. Joan Woodard	Sandia National Laboratory

Government Advisors

LTC Joe Charagua, USA	Army Reserve/OCAR
COL Bev Garrett, USA	HQ U.S. Army Pacific
LTC Charlotte Hallengren, USA	IDA

TECHNOLOGY AND SYSTEMS PANEL**Panel Co-Chairs**

Dr. Frank Fernandez	Private Consultant
Mr. Jim Shields	Charles Stark Draper Laboratory

Members

Dr. Joe Braddock	Army Science Board, OASA (RDA)
Dr. Robert Brammer	Northrop Grumman
Dr. Michael Bruno	Davidson Laboratory
Dr. Lisa Costa	The MITRE Corp.
Dr. Andrew Ellington	University of Texas at Austin

Dr. Mark Harper	U.S. Naval Academy
Mr. Art Money	Private Consultant
Mr. Walter Morrow, Jr.	MIT Lincoln Laboratory
Dr. William Rees, Jr.	Georgia Institute of Technology
Dr. Stephen Squires	Hewlett Packard Company
Dr. Jill Trehwella	Los Alamos National Laboratory
Dr. Harry Vantine	Lawrence Livermore National Laboratory
Dr. Richard Wagner	Los Alamos National Laboratory
Government Advisors	
Dr. Jane Alexander	Homeland Security Advanced Research Projects Agency
Mr. Mike Evenson	DTRA
Mr. Ben Riley	ODUSD(AS&C)
Dr. Richard Stulen	Sandia National Laboratory

EXECUTIVE SECRETARY

COL Neal Anderson, USA	NORTHCOM
Mr. Paul Bergeron	DATSD Chemical/Biological Defense
LTC Craig Costello, USA	OASD(HD)

DSB REPRESENTATIVE

LTC Scott Dolgoff, USA	DSB Secretariat
CDR David Waugh, USN	DSB Secretariat

STAFF

Ms. Marya Bergloff	Strategic Analysis
Ms. Barbara Bicksler	Strategic Analysis
Ms. Julie Evans	Strategic Analysis
Mr. Kevin Gates	Strategic Analysis
Ms. Grace Johnson	Strategic Analysis
Mr. Brad Smith	Strategic Analysis
Ms. Stacie Smith	Strategic Analysis

APPENDIX III. PRESENTATIONS TO THE TASK FORCE

January 2003

Plenary Session

Dr. Craig Fields	Summer Study Thought
Mr. Bob Saleses	Homeland Security Information Update
Mr. Bob Stoss	Office of the General Counsel Ethics Briefing
VADM Martin Mayer, USN and LTG Edward Anderson III, USA	JFCOM and NORTHCOM presentations
Dr. Randall Larsen	ANSER Perspective on Homeland Security
Ms. Anita Cohen	NIMA Homeland Security Program
VADM Lowell Jacoby, USN	DIA Perspective on Intelligence Sharing
Dr. Richard Falkenrath	Office of Homeland Security

February 2003

Plenary Session

Mr. John Gannon	Information Sharing
MG Russell Honore, USA	NORTHCOM JFHQ-HLS
Mr. Mike Wermuth and Mr. Scott McMahon	Gilmore Commission Presentation
ADM John Crowley	Department of Homeland Security
MG Raymond Rees, USA	National Guard
Mr. Thomas Reynolds	TRANSCOM: Sharing Information / Intelligence with Defense Transportation System (DTS) Commercial Partners

Mr. Raymond Geoffroy	USMC Roles and Missions in Homeland Defense
Brig Gen David Clary, USAF	Air Force Homeland Security Way Ahead
LTG William Hilsman, USA (Ret.)	National Guard Strategic Issues Task Force

Information Sharing Panel Session

COL Marenic	JREIS
Mr. Winston Wiley	Discussion
Ms. Carlynn Thompson	DTIC
Mr. Scotty Skotzko	DCI Study: Partnership and Sharing Issues between CIA and NSA
Mr. John Osterholz	Review of Data Sharing in Support of Homeland Security
Mr. Fred Turco	Information Operations
Mr. Steve Fee	JIVA Architecture

Technology & Systems Panel Session

Dr. John Carney	DARPA DSO
ADM John Poindexter, USN (Ret.)	DARPA IAO
Dr. Amy Alving	DARPA SPO
Mr. Ben Riley	ACTDs

March 2003

Plenary Session

RADM(U) Eric Olson, USN	Navy Force Protection
Mr. Dan Ostergaard	Florida Homeland Security Office
MG Tim Lowenberg, USA	Role of the National Guard in Homeland Security

Dr. Bill Weldon and CAPT Dennis Ryan, USN (Ret.) NRAC Report on Force Protection

LTG Joseph Kellogg, USA and COL Greg Gardner, USA Project Protect America

Dr. Richard Danzig Bioterrorism: What Is to Be Done?

Dr. Kevin O'Connell Public Availability of Information

Dr. John Hamre Discussion of Homeland Security Topics

Information Sharing Panel Session

Mr. Ben Riley and Mr. Jeff Gerald Homeland Security C2 ACTD

Mr. Tom Benjamin and Mr. Gilman Louie In-Q-Tel

Mr. Dave Brant Discussion

Mr. Rich Colbaugh Complex Additive Systems Analysis

Mr. John Osterholz and Ms. Marian Cherry Horizontal Fusion

Mr. Tom Mitchell and Mr. Ed Phillips CIFA Oil/Gas Pilot Brief on Critical Infrastructure Protection Discussion

BrigGen Irv Halter Overview of NRO support to Homeland Security

Mr. John Lauder NRO Comms - NRO backbone facilitating sharing of data across the community

Mr. Bob Silsby ICMAP: building the future framework of IC data sharing

LtCol Kelly Gaffney QRC - CONOPS and technologies revolutionizing overhead support

LCDR Mike Larios CMMA/BVI - Providing the current toolbox for IC/customer information sharing for ISR management

Maj Jonathan Mundt NRO Support for Analytical Tools

Mr. Jim Gosler	IO Threat Assessment
Mr. Paul Sullivan, Ms. Anjela Messer and Mr. Richard Saunders	National Guard Information Architecture
Mr. Harvey Eisenberg	Maryland Terrorism Task Force
MG Keith Alexander, USA	Discussion

April 2003**Plenary Session**

MG Craig Wheldon, USA	Hawaii Homeland Defense
Dr. David Stoudt	EMP Briefing
Mr. John Keenan	JPO-STC Critical Infrastructure Protection
COL David Barile	National Military Strategic Plan for the War on Terrorism

Information Sharing Panel Session

Mr. Rich Haver	Discussion
Mr. Rob Zitz	NIMA Innovision
Ms. Fran Townsend	USCG Intelligence

Technology & Systems Panel Session

Dr. Harry Vantine and Dr. Richard Stulen	Overview of Homeland Security Programs at Sandia and LLNL
Dr. Jill Trehwella	Overview of Homeland Security Programs at Los Alamos

May 2003**Information Sharing Panel Session**

Ms. Carol Haave	Discussion
Mr. Alan Wade, Mr. John Brennan, and Mr. Russell Travers	CIO and TTIC
Mr. Steve Dennis	Discussion

NSA

Discussions

Technology & Systems Panel Session

Dr. Richard Stulen

Systems Analysis at DoE

Dr. Parney Albright

R&D at DHS

COL Gerry Parker, USA

Army Bioterrorism Programs

Mr. Jeffrey David

TSWG

CAPT Jim Evans, USCG

Overview of Coast Guard R&D

June 2003**Plenary Session**

MG John Scott, USA

Army Communication Initiatives
Related to HLS

BG Gary Profit, USA

Army Reserve Component

Dr. John Lyons

National Academy of Sciences
Study on S&T for Army HLS

Mr. Michael Bayer

Special Study on Dirty Weapons

RADM Larry Hereth, USCG

Coast Guard - Port Security

VADM John Totushek, USN

Navy Reserve Component

BG William Rajczak, USAF

Air Force Reserve Component

MG Robert Griffin

Army Corps of Engineers

Dr. Greg Hulcher

Hard and Deeply Buried Targets

Dr. Rich Wagner

Report of the 2002/2003 DSB Task
Force on Prevention/Defense
against Clandestine Nuclear Attack

Hon. Gordon England

Department of Homeland Security
Perspective**Information Sharing Panel Session**

Mr. Paul Redmond

Discussion

Mr. Tom Lockwood and Mr. George MD's Homeland Security Advisor
Foresman

DIA

Discussions

Technology & Systems Panel Session

Dr. Tim Grayson

TTL Technologies

Dr. Robert Foster

DDR&E Perspectives on HLS

Mr. Jim Zarzycki

Programs

Biodefense Programs at Edgewood

MG J. David Bryan

DISA Cybersecurity Efforts

July 2003

Plenary Session

RDML Jim Van Sice, USCG

NORTHCOM's Road to FOC

COL Neal Anderson, USA

NORTHCOM's TOPOFF 2 Lessons
Learned

Mr. Joe Terry

NORTHCOM's Emerging Strategic
Vision

Dr. David Boyd

SAFECOM

LTG Steve Blum

National Guard Bureau

Mr. John Hathaway

Reserve Component Roles in HLS

Mr. Craig Vroom

Combined Intelligence Fusion Center

Information Sharing Panel Session

Mr. Ron Plessner

IT Privacy Issues

Technology & Systems Panel Session

COL Tim Gibson

Cybersecurity

Mr. Rich Pethia

Cybersecurity

ADM Hathaway, USCG

Coast Guard Operational
Requirements for HLS

Mr. Jay Kistler

MANPADS

APPENDIX IV. REFERENCES

- National Commission on Terrorism, "Countering the Changing Threat of International Terrorism" (The Bremmer Commission)
- Council on Foreign Relations, "America Still Unprepared- America Still in Danger" (Hart-Rudman Report)
- "CONPLAN: United States Government Interagency Domestic Terrorism Concept of Operations Plan", January 2001.
- "Third Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction" (The Gilmore Commission), December 15, 2001
- "Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction: Implementing the National Strategy" (The Gilmore Commission), December 15, 2002.
- The United States Commission on National Security/ 21st Century, "Road Map for National Security: Imperative for Change" (Hart-Rudman Commission), January 31, 2001.
- The National Security Strategy of the United States of America, September 2002. <http://www.whitehouse.gov/nsc/nss.html>
- National Strategy to Combat Weapons of Mass Destruction, December 2002.
<http://www.whitehouse.gov/news/releases/2002/12/WMDStrategy.pdf>
- National Strategy for Homeland Security, July 2002.
<http://www.whitehouse.gov/homeland/book/>
- Homeland Security Act of 2002 (H.R. 5005).
http://www.dhs.gov/interweb/assetlibrary/hr_5005_enr.pdf
- Defense Science Board 1997 Summer Study Task Force on DoD Responses to Transnational Threats, October 1997.

Republican Main Street Partnership, "A Republican Approach to the Department of Homeland Security: Recommendations for the First 100 Days", Fall 2002.

Jacoby, Vice Admiral Lowell. "Current and Projected National Security Threats to the United States: Statement for the Record, Senate Select Committee on Intelligence", 11 February 2003.

ROLES AND MISSIONS

Whelden, Major General Craig B., "Hawaii's Homeland Security" from *MILITARY REVIEW*, May-June 2002.

GAO, "Homeland Security: Management Challenges Facing Federal Leadership", December 2002.

O'Rourke, Ronald, "Homeland Security: Navy Operations-Background and Issues for Congress", Congressional Research Service Report, June 3, 2003.

Transformation Planning Guidance, April 2003.

INTERAGENCY

National Guard Bureau, "National Guard Bureau Report to Congress: Enhancing The National Guard's Readiness To Support Emergency Responders In Domestic Chemical And Biological Terrorism Defense", July, 20, 1999.

US Coast Guard, "Maritime Strategy for Homeland Security", December 2002.

INFORMATION SHARING

Defense Science Board Task Force Report on Intelligence Needs in Support of the War on Terrorism. October 2003.

Defense Science Board 2000 Summer Study on Defensive Information Operations. March 2001.

Department of Agriculture Departmental Regulation Number 3440-2, "Control and Protection of Sensitive Security Information", Dated January 30, 2003.

Department of Defense Directive Number 5230.24, "Distribution Statements on Technical Documents", Dated March 19, 1987.

Wiley, Winston P., "Joint Statement of the Terrorist Threat Integration Center Senior Steering Group"

D'Amuro, Pasquale J., Senate Governmental Affairs Committee Hearing - "Consolidating Intelligence Analysis: A Review of the President's Proposal to Create a Terrorist Threat Integration Center- Day 2", February 26, 2003

Director of Central Intelligence Directive, "Terrorist Threat Integration Center", Effective May 1, 2003.

International Association of Chiefs of Police, "Interim Report: Development of the National Criminal Intelligence Sharing Plan"

TECHNOLOGY AND SYSTEMS: CBRNE

Defense Science Board 2001 Summer Study on Defense Science and Technology. May 2002.

Defense Science Board Task Force Report on Homeland Defense Against Bioterrorism. November 2002.

NBC Defense Management. <http://www.acq.osd.mil/cp/nbc97.html>

Report on Biological Warfare Defense Vaccine Research & Development Programs, July 2001.
<http://www.defenselink.mil/pubs/ReportonBiologicalWarfareDefenseVaccineRDPgras-July2001.pdf>

National Research Council, "Science and Technology for Army Homeland Security, Report 1", 2003.

TECHNOLOGY AND SYSTEMS: CYBERSECURITY

President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructure" (Marsh Report), October 1997.

APPENDIX V. GLOSSARY OF ACRONYMS AND ABBREVIATIONS

ACTD	Advanced Concept Technology Development
AFRRI	Armed Forces Radiobiology Research Initiative
AIS	Automated Identification System
ASD(HA)	Assistant Secretary of Defense for Health Affairs
ASD(HD)	Assistant Secretary of Defense for Homeland Defense
ASD(LA)	Assistant Secretary of Defense for Legislative Affairs
ASOCC	Area Security Operations Command and Control
BCBP	Bureau of Customs and Border Protection
CapWIN	Capital Wireless Integrated Network
CBIRF	Chemical, Biological Incident Response Force
CBRNE	Chemical, Biological, Radiological, Nuclear, and High Explosives
CJCS	Chairman, Joint Chiefs of Staff
CONUS	Continental United States
DHS	Department of Homeland Security
DoD	Department of Defense
DMAT	Disaster Medical Assistance Team
DMORT	Disaster Mortuary Assistance Team
DSB	Defense Science Board
GMDSS	Global Maritime Defense and Safety System
HHS	Health and Human Services
HUMINT	Human Intelligence
IAD	Information Assurance Directorate
IND	Improvised Nuclear Device
ISR	Intelligence, Surveillance, and Reconnaissance

JCCSE	Joint CONUS Communication Support Element
JHOC	Joint Harbor Operations Center
JPO-STC	Joint Project Office-Special Technical Countermeasures
JRAC	Joint Rear Area Coordinators
MACA	Military Assistance to Civil Authorities
MCTFER	Military-Civilian Task Force for Emergency Response
MEADS	Medium-Range Extended Air Defense System
MOU	Memorandum of Understanding
NADC	North American Defense Command
NORAD	North American Aerospace Defense Command
NORTHCOM	United States Northern Command
NSA	National Security Agency
OSD	Office of the Secretary of Defense
R&D	Research and Development
RDD	Radiological Dispersal Device
SIPRNET	Secret Internet Protocol Router Network
SBU	Sensitive But Unclassified
TSA	Transportation Security Administration
TTIC	Terrorism Threat Integration Center
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
USPACOM	United States Pacific Command
WMD-CST	Weapons of Mass Destruction-Civil Support Team